Verizon 2014 PCI Compliance Report

An inside look at the business need for protecting payment card information.

In 2013, 64.4% of organizations failed to restrict each account with access to cardholder data to just one user — limiting traceability and increasing risk. *(Requirement 8)*

An executive summary of this report is available from verizonenterprise.com/pcireport/2014.

This report offers a global perspective on the state of compliance with the Payment Card Industry (PCI) Security standards, highlighting the trends and noteworthy developments across industries and regions. We also look at how compliance can be a positive force for change, improving business processes and delivering a direct return on investment (ROI).

UNIQUE INSIGHT AND ADVICE

This report offers insight into the challenges and pitfalls that you may face when striving to comply with the PCI standards, a view into the progress and evolution of those standards, and advice on how to increase the impact of your compliance initiatives. Whether you're a Chief Information Security Officer (CISO), a Compliance Officer, or a CEO, and whether you work in retail, hospitality, healthcare, financial services, or any other industry that processes card payments, this report offers you the opportunity to compare your own PCI experiences against those of other companies from around the globe.

BUILT ON A STRONG DATA FOUNDATION

This report is based on a unique dataset, including detailed quantitative results from hundreds of compliance assessments carried out by our PCI Security practice across hundreds of sites — stores, offices, data centers and even an airport. We also draw on data from our other highly authoritative security report, the Data Breach Investigations Report (DBIR).

To learn more about our approach to producing this report, see the Methodology section on page 4.

WHAT IS PCI DSS?

PCI Security standards are a set of international standards created and maintained by the PCI Security Standards Council (SSC), which represents the major card brands, to verify that merchants and service providers are appropriately protecting cardholder data. They cover all forms of payment card — debit, credit, store and company purchasing cards — carrying the logo of a PCI brand member. This represents the vast majority of payment cards issued globally.

PCI brand members: American Express, Discover Financial Services, JCB International, MasterCard, Visa Europe, and Visa Inc.

The PCI Security standards are not law (except in a couple of US states) and so non-compliance is not punishable by imprisonment; instead, it's enforced through terms of business as part of the contract between the merchant, acquirer, and other parties. Companies that choose not to comply are likely to get less beneficial commercial terms (and may even be refused service), and those that suffer a breach and are found to have fallen out of compliance are likely to face significant penalty fees.

The PCI Data Security Standard (DSS) 2.0, on which this report focuses, is a set of six objectives — broken down into 12 requirements and 289 controls and subcontrols. These controls cover everything from encrypting stored data to conducting vulnerability assessments and configuring access controls. They offer merchants a baseline for effective protection of customer payment data.

Over time the PCI Security standards have been augmented by a large number of additional templates, guidance notes, assessment criteria and other standards published by the PCI SSC. These documents are designed to be used both by organizations in their own compliance efforts, and by internal and independent assessors who evaluate each organization's compliance state annually.

CONTENTS

METHODOLOGY

Since 2009 we've performed nearly 4,000 assessments for more than 500 organizations, mainly large multinationals with complex, multi-site environments. This scale of experience is unparalleled, making the insight provided by our PCI Security and RISK teams in this report invaluable.

This research is based on quantitative data gathered by our qualified security assessors (QSAs) while performing baseline assessments on PCI DSS 2.0 compliance between 2011 and 2013. The companies that we assessed span many industries and countries.

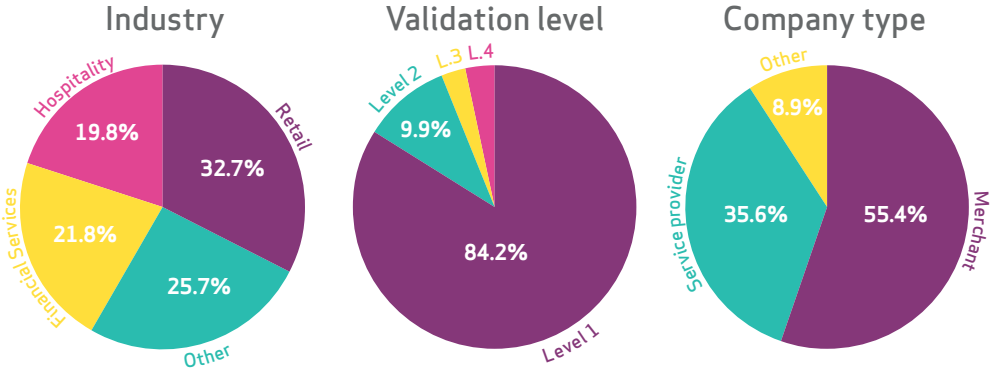


Figure 1: Breakdown of our dataset

In this report we look at:

- **Compliance by organization** — the number of companies that passed all the validation testing requirements (controls and subcontrols) that it was assessed on, divided by the total number of companies assessed. We look at this by requirement and for all requirements. Where a control or subcontrol was failed, this failure is taken to cascade upwards (so failing 3.5.2.b would lead to failing subcontrol 3.5.2, control 3.5, Requirement 3 and the whole assessment).
- **Average compliance** — the number of companies passing a specific set of controls and subcontrols (e.g., all those under Requirement 3), divided by the sum of the assessments made on that set of validation testing requirements.

All data was anonymized prior to processing to protect the privacy of the organizations involved.

Throughout this research report we'll make reference to specific requirements described in the PCI DSS 2.0 and 3.0, and related standards such as the Payment Application Data Security Standard (PA-DSS) and Point-to-Point Encryption (P2PE). These documents can be obtained from the PCI Security Standards Council (SSC) document library: pcisecuritystandards.org/security_standards/documents.php

About the authors

Lead author: *Ciske van Oosten*, Director of Operations, Verizon PCI Security practice
Ciske has been involved with PCI compliance since the very inception of the program in 2002. He established and directed the world's first QSA company, and has since served as practice leader at several QSA organizations. In these roles he's overseen more than 2,500 projects for processors, acquirers, issuers, merchants, and service providers.

He is also the author of several publications on data protection and compliance, and a well-known speaker on PCI compliance and compliance performance management — he's addressed more than 130 conferences and events in over 25 countries.

In addition to over 20 years of business experience, Ciske holds a Master's in Information Security from the University of Liverpool, an Honors Degree in Computer Auditing, a Diploma in Business Computing, and various industry qualifications such as ISO/IEC 27001 Lead Auditor, CISSP, CISM, and QSA.

Co-authors
Allen Mahaffy, Amiel DeGuzman, Gabriel Leperlier, Ian White, Jaime Villegas, Kim Haverblad, Pierre-Emmanuel Leriche, Pieter Grobler, Raul Dolado, Rein van Koten, and Ron Tosto.

Data analysis, contributors and reviewers
Aaron Reynolds, Andi Baritchi, Antonin Garcia, Bruce Forestal, David Dos Santos, Doug Smith, Eric Jolent, Franklin Tallah, Gaurav Benjamin, John Marosi, John Williams, Jyri Ryhanen, Mark Stachowicz, Matthew Arntsen, Michel Banguerski, Priyanka Bhattacharya, Rob McIndoe, Rodolphe Simonetti, Sebastien Mazas, Staci Downey, and Vincent Lucas.

This report would not have been possible without contributions of data and insight from across Verizon's QSA community and RISK team.

Verizon 2014 PCI Compliance Report
INTRODUCTION

2014 will be a pivotal year for merchants and service providers looking to comply with PCI standards.

A DECADE ON, AND MORE IMPORTANT THAN EVER

Payment card data is becoming more important as cards supplant cash, and as our DBIR data shows, it's a prime target for attackers. As we are putting the finishing touches to this report, the FBI has issued a warning to retailers to be wary of "card-targeting malware" thought to already be responsible for the breaching of over 100 million people's card data.[1]

The PCI DSS is designed to standardize and assess how organizations are protecting the card data they hold from this and other threats. The PCI Security standards apply to all organizations that handle cardholder data. The core standard, the PCI DSS, has been around for nearly a decade; and service providers, merchants, and financial companies of all sizes and from around the world have adopted it. PCI DSS is the most widespread and established standard of its kind: it's broadly accepted, widely discussed, and it's not going away.

So it's widespread. But is it effective in achieving security? Our evidence suggests that it is.

ORGANIZATIONS THAT ARE BREACHED TEND TO BE LESS COMPLIANT WITH PCI DSS THAN THE AVERAGE OF ORGANIZATIONS IN OUR RESEARCH.

As we enter the tenth year of PCI DSS, there has been important progress. With version 3.0, PCI DSS is more mature than ever, and covers a broad base of technologies and processes such as encryption, access control, and vulnerability scanning to offer a sound baseline of security. The range of supporting standards, roadmaps, guidance, and methodologies is expanding. And our research suggests that organizations are complying at a higher rate than in previous years.

After an uncertain start, many organizations now feel comfortable with and better understand what the DSS is about, and accept that complying with it is not only a necessary part of accepting card payments, but also a solid baseline of controls for protecting cardholder data.

Most analysts agree that, while the PCI standards are imperfect, they have evolved to clarify expectations and address feedback from the industry, and today they provide an increasingly mature framework for organizations to work toward.

So why is PCI compliance still worth talking, and indeed writing a major piece of research, about?

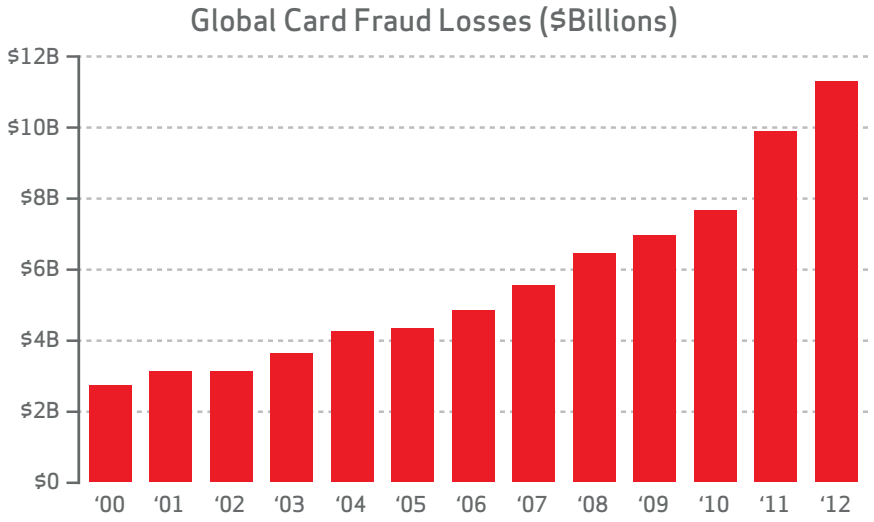


Figure 2: The cost of card fraud; data from The Nilson Report, August 2013

2014 MILESTONES

- ***The PCI Data Security Standard (DSS) turns ten years old***
- ***DSS 3.0 becomes effective and validation assessments start (January 1)***
- ***DSS 2.0 expires and compliance validation against version 3.0 becomes mandatory (December 31)***

Payment card data remains one of the easiest types of data to convert to cash, and therefore the preferred choice of criminals. 74% of attacks on retail, accommodation, and food services companies target payment card information.

Data from Verizon Data Breach Investigations Reports (DBIRs), 2011, 2012 and 2013

COMPLIANCE REMAINS A MAJOR ISSUE

But our research also shows that the vast majority of organizations are still not sufficiently mature in their ability to implement and maintain a quality, sustainable PCI Security compliance program, and they continue to struggle to provide the required compliance evidence at the time of the annual compliance validation assessment.

There's significant variation across the individual requirements, controls, and subcontrols; as well as across industries and regions. Despite a decade of discussion, clarification, and education, there are fundamental disagreements and misunderstandings around critical areas of security and compliance, including how to define the scope of compliance itself, and how compliance is assessed. Some even regard the DSS, even in its latest 3.0 guise, as taking fundamentally the wrong approach to security.

According to our research, only around one in ten organizations were fully compliant with PCI DSS 2.0 at the time of their baseline assessment. Despite the increasing maturity of the standard and organizations' understanding of it, attaining compliance remains far from easy — and so it should. Protecting cardholder data is important and the threats to it are very real.

And the drivers for investing in security and compliance are more pressing than ever. The very payment card data breaches that PCI DSS was designed to help avoid are growing in frequency and scale, with compromised records often numbering in the millions. As consumers and businesses continue to ditch cash and do more of their shopping online, the risk and impact of breaches is set to grow further. The related disciplines of security and compliance are, consequently, still a top business priority.

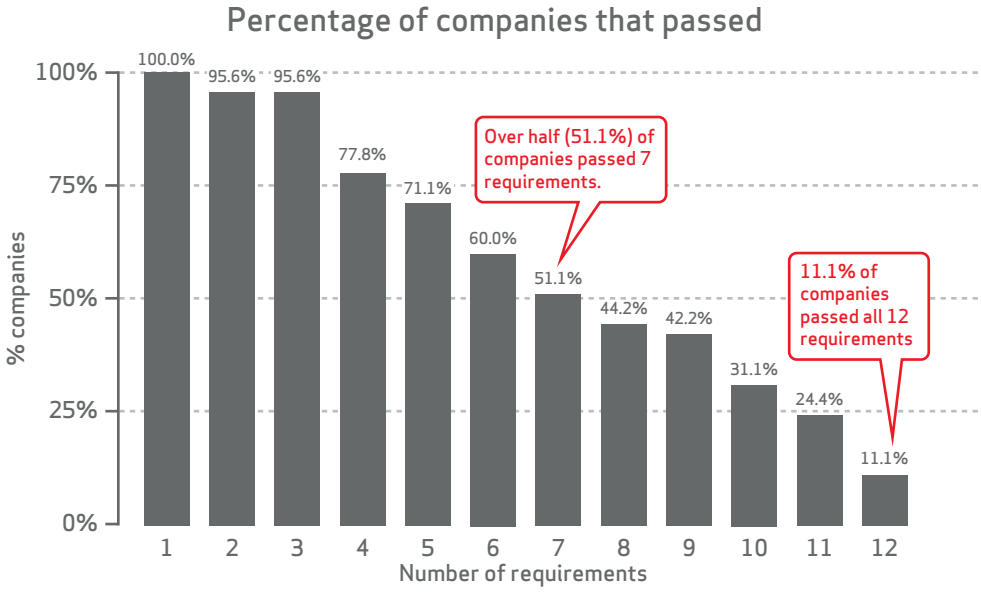


Figure 3: Percentage of companies that passed; dataset 2013

PREPARING FOR CHANGE

In many ways, PCI DSS 3.0, which became effective on January 1, 2014 and is mandatory from January 1, 2015, heralds an important shift in approach, with more new requirements and clarifications than we saw even in DSS 2.0. Our data shows that there's an initial dip in compliance whenever a major update to the standard is released — so organizations will have to put in additional effort to prepare for achieving compliance with DSS 3.0.

As a result, we think that 2014 will be a pivotal year for the PCI standards, for the organizations that strive to comply with them, and the companies that help them.

While these questions are important, they're overshadowed by one that's even more crucial to organizations around the world: how can we comply more effectively? That's the question we'll come back to time and again in this report.

Overall, we recommend five key approaches:

1 DON'T UNDERESTIMATE THE EFFORT INVOLVED

PCI compliance needs time, money, and executive sponsorship. It needs to be part of everybody's job — application developers, system administrators, executives, and even staff in shops and call centers — not just left to the IT security team.

2 MAKE COMPLIANCE SUSTAINABLE

There are thousands of tasks that an organization must complete throughout the year to stay compliant. To be sustainable, compliance needs to be embedded in "business as usual" as an ongoing process.

3 THINK OF COMPLIANCE IN A WIDER CONTEXT

The best thing you can do as an organization to simplify your PCI compliance workload and achieve real security is to put your compliance program within your wider governance, risk, and compliance strategy.

4 LEVERAGE COMPLIANCE AS AN OPPORTUNITY

Done right, PCI Security compliance can drive process improvements, identify opportunities to consolidate infrastructure, and generate additional equity. Think of it as an opportunity, not a burden.

5 FOCUS ON SCOPING

There is lots of misunderstanding around how to keep systems out of scope, but there are clear best practices to follow. The first is to store less data on fewer systems. This not only makes achieving compliance easier, it can also save you money on storage and backup.

We discuss these recommendations in more detail on page 47.

PCI Has its Critics
ARE THEY RIGHT?

Achieving consensus between hundreds of companies across many industries and countries on anything is a daunting feat to attempt. And protecting data is a complex topic with wide-reaching implications. So, it's little surprise that PCI DSS has its critics. In this section we look at the criticisms that we have encountered most often, and assess how we think the PCI SSC is doing.

"Efforts to comply distract companies from what's really important: security"

THE CRITIQUE

The standard encourages organizations to focus on compliance as a goal in itself, rather than as a means for improving the security of the cardholder data environment (CDE) against the risks that it faces. The PCI DSS doesn't drive an organization to build a comprehensive security program, it merely encourages it to achieve compliance for those systems in scope of the regulation. In fact, given the cost of complying with all the requirements specified in the standards, organizations may be discouraged from making other investments in security that could benefit their overall security posture.

OUR RESPONSE

Our DBIR research found that organizations that suffered a data breach were less likely to be PCI-DSS-compliant at the time of their breach — even if compliant at the time of their last assessment — than the average of companies assessed. While no set of security standards or technologies can eliminate the risk of a data breach entirely, we believe that organizations with security controls in place as part of complying with PCI Security standards improve their chances, both of avoiding a breach in the first place, and of minimizing the resulting damage if they are breached.

In itself, this is an important achievement and a clear answer to the many criticisms leveled at the PCI Security standards. And compared to having no such standard, it's clear that the PCI SSC has succeeded in raising the visibility of data protection issues across the industry. That said, there are several important criticisms of the PCI DSS in particular that remain open to discussion even after the enhancements, clarifications, and expansions in version 3.0.

"The PCI program doesn't address the dynamic threat environment"

THE CRITIQUE

PCI-DSS compliance is based on an annual compliance validation assessment, either an assessment by a QSA or internal security assessor (ISA), or a self-assessment questionnaire (SAQ). In between these evaluations of an organization's CDE, there's plenty of time for the business, its processes, people, and technology to change, moving the organization out of compliance and away from security best practices. The risks and threats faced by the organization are also constantly changing. While PCI DSS does require routine monitoring of the CDE, and reassessment (or at least rescanning) of the CDE after "major changes," the criteria for this trigger are ambiguous, and are fundamentally based on internal changes only.

OUR RESPONSE

If the PCI SSC tried to mandate controls on systems outside the CDE it would face a barrage of criticism. The PCI DSS 3.0 makes a clear effort to position itself as a guide or vehicle rather than as a destination. The PCI Security standards set a solid baseline for data security; organizations are free to implement this throughout their entire business – and many would benefit from doing so.

Every change, from new server deployments to new malware outbreaks, multiplies the likelihood of a breach. Thinking about security solely in terms of achieving compliance with any standard is simply not enough — organizations must take responsibility for protecting both their reputation and their customers.

Future releases of the DSS would probably benefit from having stronger integration of enterprise and operational risk management practices. That would help provide greater understanding of exposure to data breaches, increase confidence in control effectiveness, and facilitate levels of assurance.

PCI compliance shouldn't be seen as a burdensome annual ritual that the organization must endure.

"The PCI program doesn't keep up with change"

THE CRITIQUE

Updates to the PCI DSS, PA-DSS and other standards occur on a three-year cycle. This is not often enough to address the changing information security threat landscape, changing IT practices and changing consumers. Critics argue that it hasn't kept up with:

- *Advances in payment technology — such as mobile payments and increasingly sophisticated store cards*
- *The adoption of cloud and virtualization technologies by companies looking to increase agility and cut costs*
- *The increasing sophistication of hackers and the brute power they have at their disposal*

OUR RESPONSE

We don't believe that updating the standards more frequently is the answer. In fact, the release cycle shifted from the previous two-year cycle in response to feedback that organizations needed more time to learn about and comply with new versions of the standard, and to provide input and feedback to the PCI SSC.

To enhance the maturity of the corporate information security management system, and the effectiveness of the control environment, organizations are encouraged to implement additional security controls beyond those prescribed in the PCI Security standards.

Our DBIR research shows that while perpetrators are upping the ante — trying new techniques and leveraging far greater resources — less than 1% of the breaches use tactics rated as 'high' on the VERIS difficulty scale for initial compromise. In fact, 78% of the techniques we saw were in the 'low' or 'very low' categories.

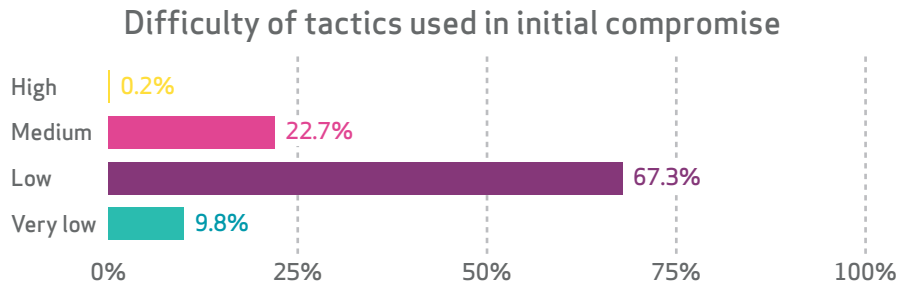


Figure 4: Sophistication of attack methods used; dataset DBIR 2013

The PCI SSC initiated several Special Interest Groups (SIGs) to provide guidance on technologies like cloud computing, virtualization, and tokenization, and other broadly applicable topics like risk assessment, maintaining PCI compliance, and third-party security assurance. It has also added multiple "best practices" to the DSS, which forward-thinking organizations can adopt before they officially come into force.

WHICH IS WORSE: OUT-OF-DATE, OR HALF-BAKED?

The PCI SSC has responded to demand for guidance on compliance in cloud environments by publishing a set of guidelines. But while in some respects well received, some analysts have called the recommendations unrealistic. For example, the guidelines demand that merchants provide logs from the cloud environment to their QSA. Critics have questioned whether cloud providers are in a position to share these logs, because they could reveal information about other users of the cloud environment. But all serious cloud providers have made great strides in addressing security concerns, and few would struggle to provide the assurances and information required by the guidelines.

"There's little attention paid to residual risk"

THE CRITIQUE

The PCI DSS fails to integrate a proper risk-based approach throughout the lifecycle of its security controls. All systems have a level of inherent risk; controls are implemented to reduce this risk, but they rarely eliminate it entirely. It's vital that the residual risk, the level of risk remaining after the controls have been implemented, is assessed. This is the only effective way to measure the effectiveness of the controls and understand what risks remain and must be managed. Until this is included within the standard, it's too easy for companies to either be unaware (in which case they will have a false sense of security) or unwilling to address these risks.

OUR RESPONSE

The standard has included an annual risk assessment requirement (as part of Requirement 12) since its inception; QSAs must verify that this assessment has been performed and a written risk assessment report created. With subsequent updates to the standard, more risk assessment requirements were added, along with important clarifications and approaches that organizations can take to satisfy their obligations. Several DSS 3.0 controls require input from the organization's risk assessment report and risk management strategy, as do decisions on the scope and implementation of a range of technical security controls.

However, despite these improvements, it's fair to say that the standard still doesn't sufficiently focus on risk measurement and management to achieve maximum effectiveness:

- While the standard suggests some industry-standard frameworks and methodologies to follow (OCTAVE, ISO 27005, and NIST SP 800-30), it does not stipulate that one must be used — without an improved definition of what a risk assessment should contain and how it should be carried out, what defines "passing" will remain highly subjective.
- It sets no requirements for the qualifications of those conducting risk assessments, or for which individuals should have the authority to accept and approve risks.
- The need for measuring and reporting on inherent risk, control risk and residual risk is not adequately described in the risk management guidance document and the standard.

Calls for a risk-based approach should not be perceived as an attempt to allow organizations to avoid implementing controls they deem irrelevant to their specific risk profile. Stronger integration of risk measurement and management, and making it an integrated part of the evaluation of control effectiveness should not result in organizations skipping required controls or bypassing the compensating controls process, but in fact make PCI DSS more relevant and effective.

It's not enough to just implement controls and think that this makes you safe. Without a well-designed and maintained risk measurement program, there's no way to reliably prove the effectiveness of your controls and the actual level of risk that remains in your business. There is a real danger in doing the minimum possible to comply. Looking back and knowing that you 'ticked the boxes' provides little comfort in the aftermath of a breach.

"The standards don't include any performance management elements"

THE CRITIQUE

PCI standards set goals and objectives for data protection controls — they give organizations a broad statement of intent and describe the specific required output that compliant organizations should achieve through their compliance program — but they fail to include guidance on performance measurement. The standards don't specify any qualitative or quantitative performance metrics an organization can use to track its activities, performance and progress toward meeting its goals.

OUR RESPONSE

Metrics are vital for managers to prove the effectiveness of their compliance initiatives, appropriately allocate resources to course-correct, and produce the data needed to demonstrate efficiency and ROI to stakeholders across the business.

As well as the costs of remediation and lost business, any organization that suffers a data breach will face a more in-depth assessment when it's time to re-validate. Most organizations are aware of this, but some still do the bare minimum needed to achieve validation. We feel that this is a shortsighted approach, and all organizations should take the security of their customers' information more seriously than this — fortunately, most do.

While the use of metrics is not a requirement for compliance, the PCI SSC encourages organizations to implement a program to measure their security and compliance capabilities and performance.

The current lack of published performance management guidance from the PCI SSC means that organizations lack clear guidance on how metrics should be used to improve their data protection capabilities. A true lifecycle approach would involve ongoing measurement of the organization's performance on:

- Discovery of what data and assets the organization has, and when and how they move
- Understanding of the risks the organization's data and assets face
- Selection, implementation, and maintenance of controls to form a sustainable control environment

This would help organizations to identify, track and report on their progress, and go a long way in helping them to be more proactive and effective at compliance maintenance.

The PCI DSS sets goals and objectives, but doesn't specify qualitative or quantitative metrics that organizations can use to measure their performance. Without clear measurement, it's harder for organizations to monitor progress and achieve continuous improvement.

"PCI-DSS assessments lack sufficient validation"

THE CRITIQUE

Only the largest merchants, processing millions of transactions each year, are required to produce a final annual report on compliance (FRoC). Smaller merchants need only complete an annual self-assessment questionnaire and satisfy the regular vulnerability scans as part of DSS Requirement 11. While most merchants strive to comply in good faith (and protect their customers' data), the lack of validation is a real problem. Internal assessors are likely to have less experience with PCI Security compliance validation than a QSA, and may come under pressure from the rest of the business to keep the burden and cost of compliance down by fudging assessments.

OUR RESPONSE

While it's potentially unfair and undesirable to burden smaller organizations with a full-blown assessment by a QSA, continued education is essential to ensure they understand their responsibility to protect cardholder data. The same PCI Security requirements apply to all merchants, large and small, and it is only the compliance validation requirements that are reduced for small merchants.

While most merchants are striving to comply in good faith, the lack of validation can be a problem.

Some merchants are not aware of this difference between the scope of compliance, and the scope of validation, particularly when newly exposed to the PCI Security regulation. This sometimes results in them focusing on controls that are tested during the validation assessment and giving less attention to the implementation of sustainable controls for the entire set of applicable requirements.

QSAs can't provide a 100% complete validation, because:

- They're assessing a selected sample, not the entire environment; they gather evidence that provides a reasonable basis for forming an opinion
- The choice of samples, and the nature, timing and extent of evaluations, is a matter of judgment
- The evidence gathered — which may include a huge volume of log files, reports, policy documents, standards, code, and assessments — must be interpreted against the individual QSA's understanding of the standard, and the context of the merchant's control environment

Given all of these variables, what is realistically achievable is "reasonable assurance" that CHD is adequately protected. In any case, it should be clear that no standard provides absolute coverage or protection, and that no type of validation will be infallible. PCI compliance validation is intended to provide reasonable, independent, unbiased assurance that an organization is meeting the baseline standard established by the industry for the protection of payment card data.

So, will DSS 3.0 fix everything?

The PCI SSC has stated that the changes in DSS 3.0 are designed to, "help organizations take a proactive approach to protect cardholder data that focuses on security, not compliance, and makes PCI DSS a business-as-usual practice." The key themes are improving education and awareness, and increasing flexibility, and viewing security as a shared responsibility.

But when the PCI SSC launched PCI DSS 3.0 in November 2013, some in the industry were disappointed that it didn't go further to address the criticisms we've discussed — and others.

One of the most important changes in DSS 3.0 is how it specifies that organizations must map out their CDE, following the flow of cardholder data (CHD). But while this is an important part of defining scope and identifying risk and vulnerability, the DSS does not mention any automated means of performing this data discovery — including data loss prevention (DLP) solutions.

Perhaps most importantly — aside from improved physical security requirements, enhanced penetration testing, and vulnerability management — DSS 3.0 fails to embed its list of security controls within a full program of ongoing security governance, business continuity, and management. Organizations will benefit from making compliance activities part of business as usual, but are likely to require guidance about the assessment, management, change control, and incident response activities that help them run their security and compliance programs. Closer alignment with, or references to, information security governance and management quality standards — and in particular, the inclusion of a maturity model — would help to address this.

However, we feel that as organizations begin to prepare for validation, they will start to realize how significant a step forward DSS 3.0 is. For most organizations, achieving validation will involve significant new challenges.

We look at the changes and their implications in detail in the coming pages.

It's important to remember that while validation of compliance for attestation purposes (passing the annual assessment) is a "point in time" activity, PCI Security regulation requires full compliance to be actively maintained on a day-to-day basis.

The State of PCI-DSS Compliance

IMPORTANT PROGRESS; ROOM FOR IMPROVEMENT

In 2013 we saw a significant increase in compliance, but still only 11.1% of organizations complied fully.

11.1%

OF COMPANIES MET ALL THE DEMANDS OF DSS 2.0 IN 2013, AN INCREASE OF 3.6 PERCENTAGE POINTS ON 2012.

85.2%

IN 2013, COMPANIES WERE COMPLIANT WITH AN AVERAGE OF 85.2% OF CONTROLS.

MUCH HAS BEEN ACHIEVED...

In 2013, 11.1% of organizations were fully compliant with the standard at the time of their annual baseline assessment, up from just 7.5% in 2012.

DSS 2.0 (All requirements): Compliance snapshot

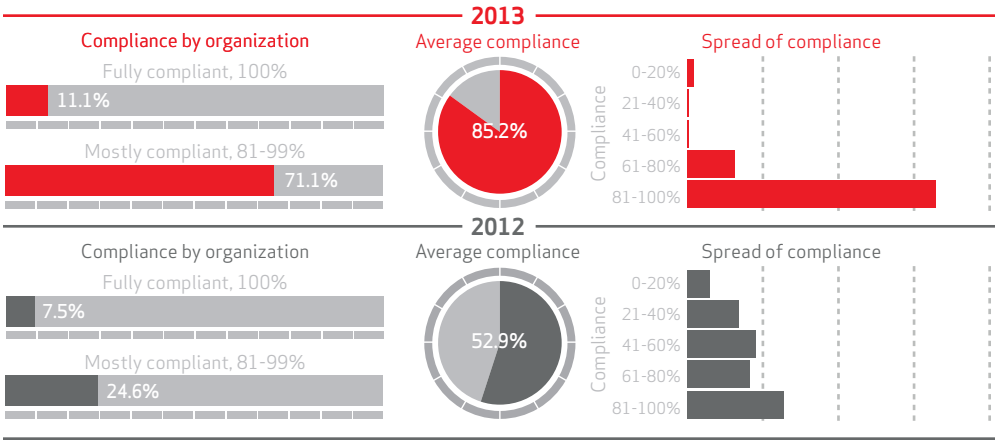


Figure 5: Snapshot for all requirements; dataset 2012 and 2013

This is still a very low figure, so we also looked at the percentage of organizations compliant with at least 80% of the controls and subcontrols. This showed a far greater increase: from just 32.1% (24.6% + 7.5%) in 2012, to 82.2% (71.1% + 11.1%) in 2013. It's worth noting that four in five organizations were "nearly there" (see figure 5).

Around one in five organizations came close to complying — they passed 95%+ of controls. Of these organizations, more than half failed Requirement 11 [Regularly test security systems and processes].

What caused this increase? We've identified three likely contributing factors:

- **Increased awareness about PCI:** Efforts by the PCI SSC, the card brands, and security vendors have paid off. PCI compliance has become a regular topic of discussion in organizations, on the Internet, and in business and technology media. IT and business leaders understand the data protection and compliance landscapes better than ever.
- **Increased appreciation for the value of PCI compliance:** The attention given in the mass media to data breaches has brought data protection to the forefront. The consequences of data breaches, and the value of implementing effective security controls, are better understood and appreciated across the business.
- **Increased maturity in the security standards:** Each of the five updates to the DSS has addressed ambiguity and improved clarity around the interpretation and intent of the security controls. The security industry responded to improve existing security technology and develop new solutions where needed to address the changing risk and compliance landscape.

...BUT IT'S NOT ALL GOOD NEWS

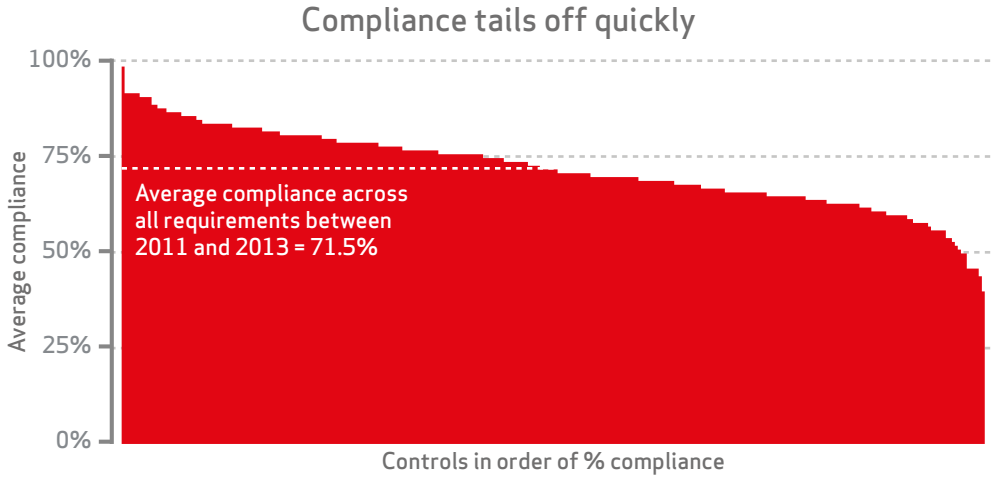


Figure 6: Controls in descending order of compliance; dataset 2011-2013

While the picture is very encouraging at a macro level, looking more closely at the data reveals significant variations:

- **Requirement to requirement:** From 2011 to 2013, 58.4% of organizations complied with all the controls of Requirement 7 [Restrict access to cardholder data by business need to know], but just 23.8% with those of Requirement 11 [Regularly test security systems and processes]. Looking solely at 2013, 91.1% of organizations in our study complied with at least 80% of the controls of Requirement 5 [Use and regularly update anti-virus software or programs]; just 68.9% with those of Requirement 11. The number of organizations compliant with at least 80% of the controls in Requirement 11 increased by 50 percentage points (18.9% to 69.9%) between 2012 and 2013; the same figure for Requirement 4 was just 21 percentage points (54.7% to 75.6%).
- **Industry to industry:** Twice as many retailers were compliant with at least 80% of all 289 controls as hospitality organizations, 69.7% versus 35.0%.
- **Region to region:** In Europe, just 31.3% of organizations were compliant with at least 80% of controls, lagging the North America (56.2%) and Asia-Pacific regions (75.0%).

31.3%

OF EUROPEAN ORGANIZATIONS COMPLIED WITH 80%+ OF DSS 2.0 CONTROLS, LAGGING THE NORTH AMERICA (56.2%) AND ASIA-PACIFIC (75.0%) REGIONS.

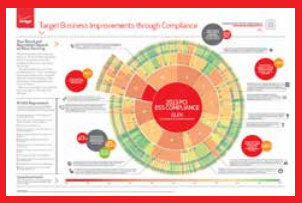
Summary of compliance by requirement

(l) = lowest (h) = highest

Req	Fully compliant		Mostly compliant		Average compliance	
	2012	2013	2012	2013	2012	2013
1	26.4%	64.4% ▲	17.0%	8.9% ▼	55.0%	86.4% ▲
2	22.6%	51.1% ▲	18.9%	20.0% ▲	53.9%	81.4% ▲
3	17.0%	68.9% ▲	13.2%	6.7% ▼	45.5%	79.3% ▲
4	34.0%	68.9% ▲	**(h) 20.8%**	6.7% ▼	61.2%	87.8% ▲
5	30.2%	80.0% ▲	17.0%	11.1% ▼	64.3%	95.9% ▲
6	22.6%	68.9% ▲	13.2%	13.3% ▲	51.4%	87.4% ▲
7	**(h) 41.5%**	73.3% ▲	11.3%	4.4% ▼	**(h) 66.6%**	86.8% ▲
8	22.6%	62.2% ▲	**(h) 20.8%**	15.6% ▼	58.0%	84.1% ▲
9	35.8%	**(h) 86.7%** ▲	15.1%	**(l) 4.4%** ▼	61.9%	**(h) 94.9%** ▲
10	20.8%	60.0% ▲	17.0%	17.8% ▲	46.9%	82.2% ▲
11	**(l) 11.3%**	**(l) 40.0%** ▲	**(l) 7.5%**	**(h) 28.9%** ▲	**(l) 38.9%**	**(l) 74.6%** ▲
12	30.2%	73.3% ▲	13.2%	11.1% ▼	54.8%	89.7% ▲
Overall	7.5%	11.1% ▲	24.6%	71.1% ▲	52.9%	85.2% ▲

Figure 7: Summary by requirement; dataset 2012 and 2013

Too many numbers? Why not download our visualization of the entire dataset? Visit verizonenterprise.com/pcireport/2014



The following pages give a detailed analysis of what we've learned about compliance with each of the 12 requirements of PCI DSS 2.0. Along with evaluating how well organizations are complying with each requirement and why, we explore why each requirement is important as part of a comprehensive security and compliance program.

We also look at the major changes between DSS 2.0 and DSS 3.0.

Despite the number of validation testing requirements per requirement varying from 6 (Requirement 5) to 40 (Requirement 12), we found no correlation between this and the level of compliance across our whole 2011-2013 dataset.

Average compliance by requirement

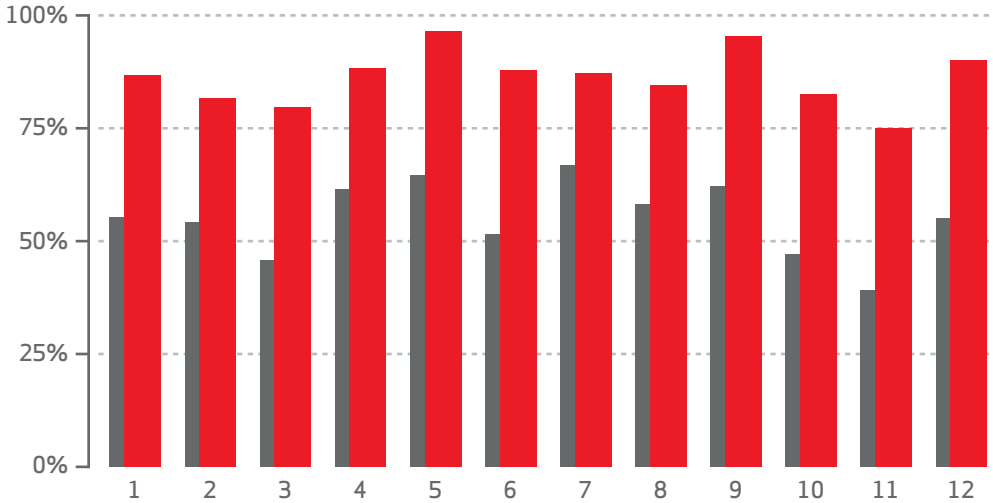


Figure 8: Average compliance by requirement; dataset 2012 (gray) and 2013 (red)

Throughout the coming sections we'll refer to our "Top 20" and "Bottom 20" lists. Shown below, these consist of the 20 most- and least-often complied-with controls and subcontrols in our entire 2011-2013 dataset.

Top 20

Rank	Control	% complying
1	2.4	98.0%
2	8.5.10.b	91.1%
3	8.5.12.b	91.1%
4	8.5.13.b	91.1%
5	8.5.9.b	91.1%
6	9.1.3	91.1%
7	2.2.3.a	90.1%
8	8.4.b	90.1%
9	8.5.11.b	90.1%
10	8.5.7	90.1%
11	9.1.2	88.1%
12	9.3.3	88.1%
13	3.4.1.b	87.1%
14	3.4.1.c	87.1%
15	9.3.1	87.1%
16	2.1.1.e	86.1%
17	3.2.a	86.1%
18	3.4.1.a	86.1%
19	5.1.1	86.1%
20	9.3.2.b	86.1%

Bottom 20

Rank	Control	% complying
270	8.5.1	57.4%
271	11.5.a	56.4%
272	10.4.1.a	55.4%
273	10.4.2.a	55.4%
274	11.3.c	55.4%
275	12.9.4	55.4%
276	2.2.2.a	55.4%
277	11.2.1.c	53.5%
278	12.1.2.b	53.5%
279	1.1.6.b	52.5%
280	2.2.2.b	51.5%
281	11.3.2	50.5%
282	11.3.1	49.5%
283	6.1.a	49.5%
284	11.2.1.a	45.5%
285	11.2.1.b	45.5%
286	11.2.3.a	45.5%
287	11.2.3.b	45.5%
288	11.3.b	43.6%
289	11.3.a	39.6%

Figure 9: "Top 20" and "Bottom 20" lists; dataset 2011-2013

REQUIREMENT 1

Install and maintain a firewall configuration to protect cardholder data

WHY IS IT IMPORTANT?

Requirement 1 helps ensure that firewalls and any other system components providing similar functionality are configured in line with documented standards.

Organizations need to protect the perimeter of their networks if they're to prevent unauthorized parties from illicitly obtaining information including CHD. A properly configured firewall is an essential part of the first line of defense. Firewall rules examine traffic and block transmissions that don't meet specified security criteria, helping to prevent network intrusions. When ongoing management and maintenance of firewall and router configurations is neglected, it can significantly increase the organization's exposure and reduce the security of the CDE.

However, it's important to note that organizations shouldn't rely solely on firewalls, or any perimeter security technology, to protect their data. And they should recognize that if firewall configurations prove difficult to penetrate, attackers are likely to move on and target other vulnerabilities in the environment — for instance, applications.

HOW DOES THIS REQUIREMENT RELATE TO SECURITY THREATS?

Data from Verizon's RISK team showed that only 12.5% of organizations that suffered a data breach in 2013 were compliant with Requirement 1 at the time of their breach. By comparison, our QSAs found an average of 46.7% compliance with Requirement 1 in the same year. This shows a strong correlation between a badly configured firewall and the likelihood of a security breach.

THE STATE OF COMPLIANCE

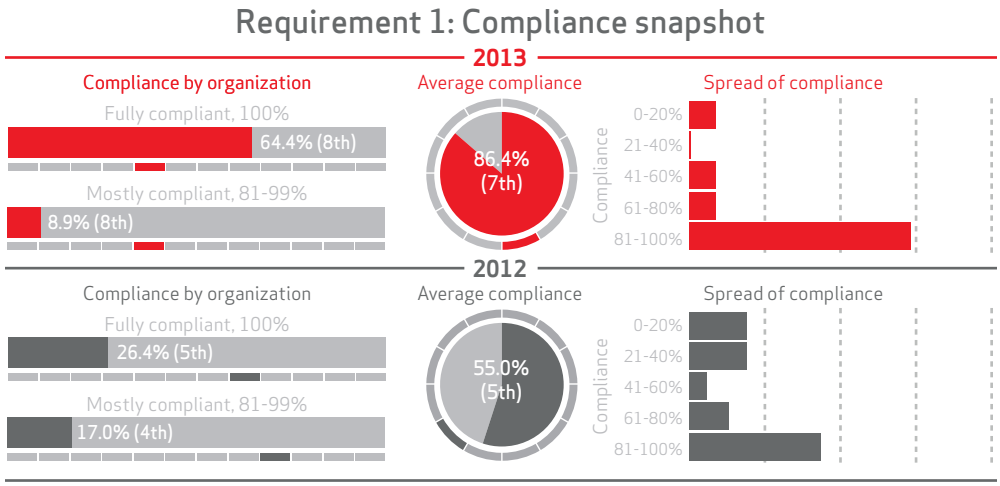


Figure 10: Snapshot for Requirement 1; dataset 2012 and 2013

For the individual subcontrols of Requirement 1, most organizations ranked high in addressing the simplest ones, like 1.1.3.a, 1.2.1.b, and 1.3.6. These subcontrols cover basic security practices that organizations usually have in place already — like including a firewall at each Internet connection, denying inbound and outbound traffic that is not necessary for the CDE, and ensuring the firewall performs deep-packet inspection.

However, compliance for subcontrols 1.1.5 and 1.1.6.b was considerably lower. These cover the documentation and reviewing of firewalls and routers, rather than the technical aspect of configuration. Detailing a review of thousands of firewall rules is a resource-intensive task — and is therefore relatively difficult to do. In fact, compliance with 1.1.6.b was so low that it appears in our "Bottom 20" list with just 52.5% of companies complying.

This requirement covers the correct usage of a firewall to filter traffic as it passes between internal and external networks, as well as traffic to and from more sensitive areas within the company's internal networks.

64.4%

OF COMPANIES MET ALL THE DEMANDS OF REQUIREMENT 1 IN 2013, AN INCREASE OF 38.0 PERCENTAGE POINTS ON 2012.

86.4%

IN 2013, COMPANIES WERE COMPLIANT WITH AN AVERAGE OF 86.4% OF CONTROLS.

Attackers have moved from targeting servers to targeting the applications they run. Criminals are now launching attacks that exploit weaknesses in HTTP and XML implementations to circumvent increasingly robust perimeter defenses. In response, the security industry has developed next-generation or application-aware firewalls. The use of these improved devices is growing, but due to lack of understanding and poor implementation, few are exploiting the full potential of this new technology.

The DSS still specifies stateful-inspection firewalls, first launched in 1994. As the threats to the CDE become more complex, these devices are less able to identify all unauthorized traffic and often get overloaded with thousands of out-of-date rules. To address this, vendors are now offering "next generation" firewalls that can validate the traffic at layers 2 to 7, potentially allowing far greater levels of granularity in the rules. Many of these devices integrate a number of network controls — for example firewall, intrusion prevention system (IPS), and malware detection — into a single platform, allowing any potential threats detected by one component to trigger changes in the behavior of the other components, and a more thorough analysis.

CHALLENGES AND PITFALLS

A problem regularly encountered during PCI-DSS assessments is firewalls and routers being configured more "generally," allowing a wide range of ports to ensure that applications function.

Members of staff often do this because they lack a clear understanding of the CHD flow or the applications and services enabled on in-scope systems, and are therefore reluctant to risk blocking a legitimate business process. Organizations need a reliable inventory of in-scope systems to accurately configure the firewall to the cardholder environment. In order to do so, they need to bring business process design, application development, and infrastructure teams together to clearly document and understand the flow of information.

Even organizations that do invest in mapping their systems and data flow often treat it as a one-off activity. Rule sets are defined at project stage and seldom updated once the project is moved to operations. Very few of these organizations have implemented the necessary review of firewall rules and after a couple of years it's nearly impossible to find the business justification for them. An analysis of the initial architecture design and all the following changes is then required to justify the existing rules. Instead, organizations should review rulesets and configurations regularly, and document modifications with a change-management procedure.

HOW IS THIS REQUIREMENT EVOLVING?

Many of the changes to Requirement 1 in DSS 3.0 are intended to clarify the language so organizations can better understand what is needed for compliance. For example, in DSS 3.0, control 1.1 adds emphasis on implementing as well as documenting firewall and router standards.

Several subcontrols have also been added to assist organizations in understanding the flow of data into and out of their environments. For example, 1.1.2 states that organizations must now produce a network map showing all the different hardware and software within the cardholder data environment. And subcontrol 1.1.3 states that organizations must produce a cardholder data flow map, which outlines where data originates in the network, how it is processed, and where it is sent out of the environment. These changes force organizations to better identify where cardholder data is stored, processed or transmitted. Using the information gathered from network assessments and from the maps themselves, organizations can create more precise firewall rules — better securing the perimeter.

DSS 3.0 control 1.4 clarifies the firewall control requirements for mobile devices — including those owned by employees — that can connect to both the Internet and the cardholder environment. When connecting via the corporate environment, access to open public networks can be controlled — multiple layers of security can be applied that can block unauthorized traffic and identify malware and prevent it from reaching the device. However if a mobile device has unrestricted access to the Internet or other public network, then there is a significant risk it could become infected. The malware would have bypassed the corporate network controls, and the whole CDE could be at risk when that device is reconnected.

REQUIREMENT 2

Do not use vendors' default passwords or security parameters

WHY IS IT IMPORTANT?

Vendor default settings, particularly passwords, are well-known by attackers; changing them at the time of installation is a simple and easy-to-implement process to harden production systems.

Requirement 2 also aims to standardize configurations and configuration-management procedures. By completely defining and documenting the expected hardened configuration of each system, and adopting tools to automate that configuration, organizations can validate that settings have been consistently applied and avoid exceptions caused by manual configuration. This can help to reduce the workload involved in administering IT infrastructure, and can also reduce the cost of compliance assessments — the QSA can verify this automation and potentially reduce the size of the validation sampling.

HOW DOES THIS REQUIREMENT RELATE TO SECURITY THREATS?

Our 2013 DBIR research found that attackers typically take the path of least resistance. Vendor-default passwords and user accounts provide the simplest possible way into a system — whether a laptop, server, or network appliance — enabling attackers to gather data directly, deploy malware, or attack other systems.

When our RISK team investigated data breaches during 2011–2013, they found that only 38.8% of organizations suffering a breach had Requirement 2 in place.

THE STATE OF COMPLIANCE

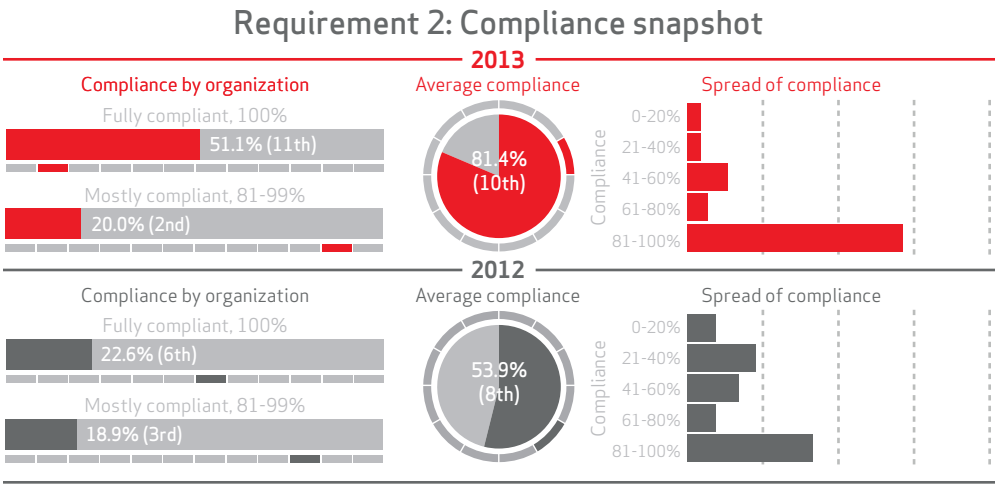


Figure 11: Snapshot for Requirement 2; dataset 2012 and 2013

Of the individual subcontrols, 90.1% of assessed organizations managed to comply with 2.2.3.a, which involves verifying that system administrators and security managers have knowledge of common security parameter settings for system components. This was the seventh-most complied-with control in the entire PCI DSS. This is an easy requirement to validate during the onsite visit, and most qualified IT staff should be able to answer the validation interview questions about the controls in place for the system in question.

At the other end of the spectrum, organizations struggled with subcontrol 2.2.2, with just 50.5% of companies complying with both of its subcontrols — each of which is in our "Bottom 20" list.

Only 55.4% of companies were in compliance with 2.2.2.a. This subcontrol requires that organizations document all services and protocols enabled on their system components, justify why they're active, and verify that controls are implemented. Administrators didn't always realize that insecure protocols were being used, as they weren't the application owners. Other times, due to the usage of legacy systems, insecure protocols needed to be used and compensating controls needed to be documented — for instance, having additional strong access controls (Requirement 8) and properly configured firewalls (Requirement 1).

This requirement covers the controls that reduce the available attack surface on production systems by removing unneeded services, functionality, and user accounts, and by changing insecure vendor default settings.

51.1%

OF COMPANIES MET ALL THE DEMANDS OF REQUIREMENT 2 IN 2013, AN INCREASE OF 28.5 PERCENTAGE POINTS ON 2012.

81.4%

IN 2013, COMPANIES WERE COMPLIANT WITH AN AVERAGE OF 81.4% OF CONTROLS.

With the uptake of virtualization, data stored only "in memory" can now easily be retained on non-volatile storage when virtual systems are suspended or snapshots are taken. This poses new threats to the security of encryption keys kept in memory in virtualized environments.

And just 51.5% of companies complied with 2.2.2b, indicating that organizations still find it challenging to provide valid business justifications for the use of insecure services, daemons, and protocols, and presenting the documentation for it.

Subcontrols 2.2.a and 2.2.b require that organizations have system configuration standards and that they are applied when new systems are configured; only 50.5% of organizations assessed had both of these controls in place (59.4% and 59.5% respectively). In our experience, system administrators are usually so busy that proper and thorough documentation of configuration standards is not seen as a priority.

CHALLENGES AND PITFALLS

It's common for organizations to struggle to meet subcontrol 2.2.4.b [Verify enabled functions are documented and support secure configuration]. Often the list of services running, which is obtained from the samples taken during an assessment, does not match what is documented.

Requirement 2 covers the configuration of all systems within the CDE. This makes it one of the requirements most affected by the emergence of virtualization and cloud technologies. These technologies simplify the way in which organizations run their IT infrastructure. However, with new technology always come new challenges, like how to segment mixed environments (in-scope and out-of-scope systems hosted in the same physical server) to prevent attacks based on shared resources or other out-of-band channels, among others.

It's worth noting that required controls cannot be used as compensating controls; an entirely new approach is required.

Some retail organizations have started to pilot mobile payment applications in their environments. However, the PCI SSC stopped all PA-DSS certification reviews for mobile payment applications in 2011. The implications are that organizations using unvalidated mobile payment applications will have a very hard time passing PCI assessments, since compensating controls are much harder to implement in mobile devices due to their limited capabilities (the reason why the PCI SSC suspended all reviews for these devices). The way around this, according to the PCI SSC, is to use P2PE solutions where mobile devices can act purely as communications devices for the encrypted traffic.

HOW IS THIS REQUIREMENT EVOLVING?

DSS 3.0 provided some changes and clarifications to existing wording, and added control 2.4, which requires organizations to maintain an inventory of system components in scope. This mirrors similar guidance in other requirements. Another new control, 2.5, requires organizations to document and communicate the policies and daily operational procedures associated with vendor defaults to responsible personnel, helping to prevent insecure configurations.

Some organizations skip requirements relating to wireless and virtualization technologies — for example, all five subcontrols of 2.1.1 were not applicable for 51.5% of companies because their CDE did not have any wireless access points. As wireless technologies and security standards continue to evolve, the DSS is changing to keep pace — we saw changes to 2.1.1 in both DSS 2.0 and 3.0.

REQUIREMENT 3

Protect stored cardholder data

WHY IS IT IMPORTANT?

Attacks on an organization's systems are often perpetrated with the aim of extracting cardholder data: it's a prime target. Stored cardholder data — whether archived long-term or cached temporarily while in use by an application — must be protected continuously, otherwise it's vulnerable to attack. Requirement 3 stipulates that organizations must never store sensitive authentication data like the card verification values (CVV/CVV2) or PINs after authorization of the transaction, even if encrypted; and render PANs unreadable using encryption, truncation, tokenization, masking (when displayed), or hashing.

HOW DOES THIS REQUIREMENT RELATE TO SECURITY THREATS?

According to the 2013 DBIR, of all the breaches studied by the Verizon Investigative Response team, not a single one involved cardholder data "in transit" between systems. However, two-thirds of data breaches involved data "at rest."

This requirement specifically covers the storage of cardholder data on system components, such as servers and databases. It states that all stored data must be protected using appropriate methods, no matter what type of system it is stored in.

Simple rule: If you don't need it, don't keep it.

When our RISK team investigated data breaches during 2011–2013, they found that 18.2% of organizations suffering a breach had Requirement 3 in place. Over the same period, our QSAs found that 32.7% of companies passed Requirement 3. This suggests some correlation between not having strong data protection methods in place and suffering a data breach.

68.9%

OF COMPANIES MET ALL THE DEMANDS OF REQUIREMENT 3 IN 2013, AN INCREASE OF 51.9 PERCENTAGE POINTS ON 2012.

79.3%

IN 2013, COMPANIES WERE COMPLIANT WITH AN AVERAGE OF 79.3% OF CONTROLS.

THE STATE OF COMPLIANCE

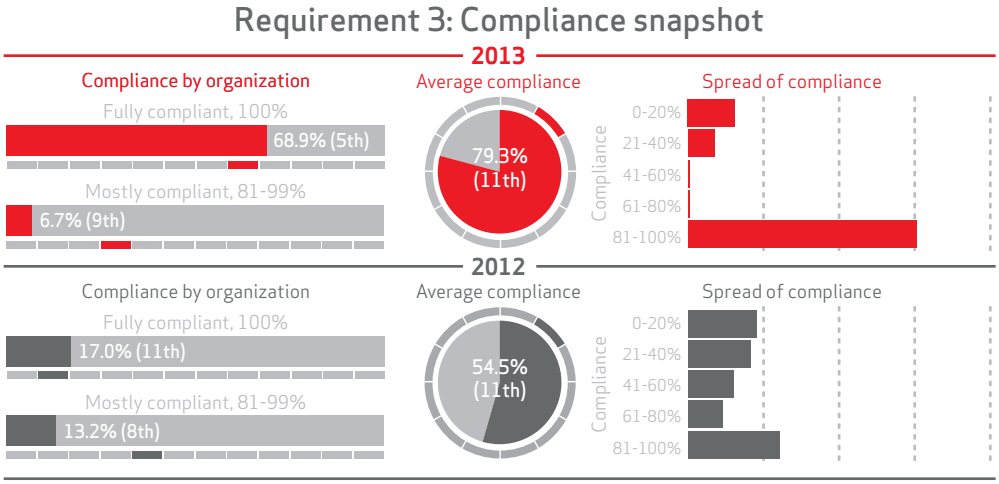


Figure 12: Snapshot for Requirement 3; dataset 2012 and 2013

Reasons for the massive increase in compliance with this requirement between 2012 and 2013 include:

- **Better tools:** Improvements in the effectiveness of automated scanning tools — particularly cutting the number of false-positives — and the consequent increase in the use of these tools.
- **Consolidation:** Better scope reduction — by cutting the number of systems that store CHD through consolidation of databases, backup systems and paper repositories.
- **Outsourcing:** Increased use of third parties, reducing the amount of data processed and stored by the organization.

Another contributing factor to the significant improvement in Requirement 3 is that nearly a third of its controls and subcontrols fall in milestone one of the PCI-DSS's prioritized approach (it makes up 60% of the controls within milestone one). We have seen acquirers using this supporting document as a roadmap for merchants to achieve compliance, with dates set to achieve each milestone.

Data "at rest" is an easier target in several ways. It often has a larger window of exposure compared to data being transmitted, "data in motion".

Interestingly, retail organizations performed significantly better than hospitality companies. Many organizations failed to comply with 3.4, which demands that they confirm that the PAN is rendered unreadable via hashes, truncation, strong encryption or tokenization. Just 47.5% of companies were compliant with all four validation testing requirements:

- 3.4.a: Obtain and examine documentation about the system used to protect the PAN, including the vendor, type of system/process, and the encryption algorithms (59.4%).
- 3.4.b: Examine several tables or files from a sample of data repositories to verify the PAN is rendered unreadable — that is, not stored in plaintext (64.4%).
- 3.4.c: Examine a sample of removable media (for example, backup tapes) to confirm that the PAN is rendered unreadable (74.3%).
- 3.4.d: Examine a sample of audit logs to confirm that the PAN is rendered unreadable or removed from the logs (70.3%).

CHALLENGES AND PITFALLS

Data "at rest" is an easier target in several ways. It often has a larger window of exposure compared to data being transmitted, "data in motion". This problem is exacerbated by a lack of understanding of all the places within the organization where CHD is stored, sometimes even in plain text. This has led many in the industry to call for a "Requirement 0," mandating automated data discovery. This would alleviate the issue of organizations only looking at data in locations where it's supposed to be — within the existing card data environment — and neglecting to confirm that card data is not present elsewhere. This isn't a requirement yet, but we'd recommend that organizations adopt this approach to keep their customer's data is safe and simplify their compliance maintenance efforts.

As noted in our analysis of Requirement 1, one of the foundations for effective PCI compliance is to accurately know how and where card data flows through various systems — from its creation to its destruction. This is why it's critical to identify and examine all desktops, laptops, and servers that handle cardholder information. This includes database files that contain card numbers, and any application system that accesses cardholder data. And it also means understanding not just databases and file stores where data is permanently stored, but also the caches and temporary files where data resides during processing.

This is challenging enough in conventional IT environments. Mobile devices, particularly those brought into offices, retail sites, and other environments by employees as part of the "bring your own device" trend, make it even more difficult. Mobile devices running a range of operating systems, applications, and services require different tools to manage and may not support appropriate device management controls, including strong encryption and logging.

New forms of attack are emerging that target data during processing and transmission — partly driven by increasing security measures put in place to protect data at rest. The PCI DSS does not currently require organizations to encrypt data being transmitted within the CDE. We believe that unless this is addressed, it could become a significant threat to CHD.

HOW IS THIS REQUIREMENT EVOLVING?

Many of the changes introduced to Requirement 3 in DSS 3.0 involve improving the management of encryption keys. Subcontrol 3.5.1 covers restricting access to keys to the minimum possible number of people, and 3.5.3 requires that keys are stored in as few places as possible. The subcontrols under 3.6 mandate that best practices are followed when replacing keys when they reach the end of their life or are compromised, and that those entrusted with managing keys understand and accept their responsibilities.

DSS 3.0 also clarifies the principles of split knowledge and dual control. Split knowledge is a method in which two or more people separately have key components, and each person knows only their own key component. Dual control requires two or more people to perform a function, and no single person can access or use the authentication materials of another person.

Control 3.2 has been updated to require that all data is rendered unrecoverable upon completion of the authorization process, clarifying the intent.

REQUIREMENT 4

Encrypt transmission of cardholder data across open, public networks

WHY IS IT IMPORTANT?

The encryption of data transmissions is a foundational information security practice, and most IT departments are familiar with how to protect common systems and applications. Requirement 4 covers communications over public/open networks, including email sent to and from the organization (e.g. in communications between customers and service staff) and transactions made over the Internet.

It is essential to use suitable data protection technology (such as secure SSL or TLS) to encrypt communications containing cardholder data that take place over any untrusted network, including internal ones. The term "untrusted network" includes any network outside of the organization's control, like the Internet, and local "over the air" networks, like Wi-Fi and Bluetooth — even if they belong to the organization.

HOW DOES THIS REQUIREMENT RELATE TO SECURITY THREATS?

Attackers know that CHD sent over open/public networks is usually well protected, and therefore go after softer targets — of all the incidents our RISK team investigated and reported upon in the 2013 DBIR, not one breach involved data "in transit." In two-thirds of breaches data was compromised at rest (see Requirement 3, page 21); the remaining cases occurred during processing. But this is no reason to be complacent, especially with more people using their own devices and working from home — potentially accessing all kinds of unsecured networks.

THE STATE OF COMPLIANCE

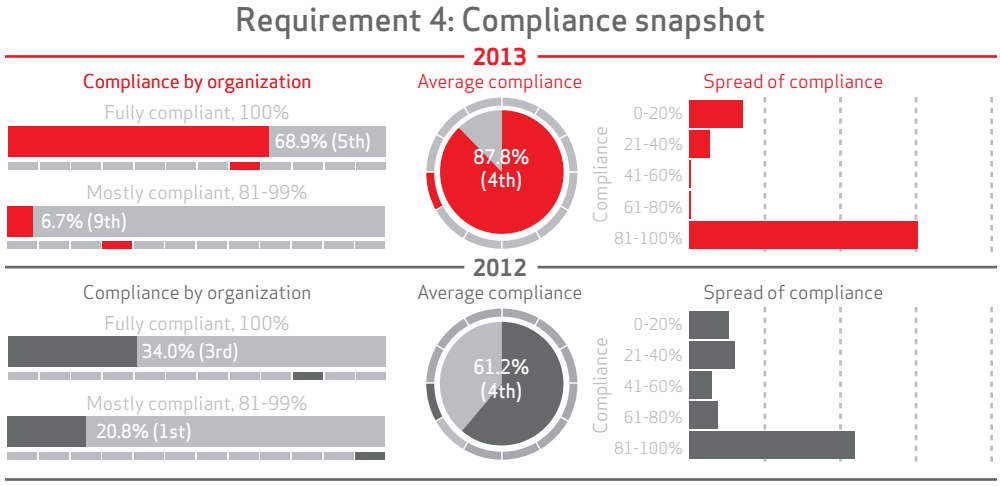


Figure 13: Snapshot for Requirement 4; dataset 2012 and 2013

The most-often complied-with subcontrols included 4.1.b on the use of trusted keys and certificates (84.2%) and 4.1.e on using HTTPS in web sessions (83.2%).

The least complied-with subcontrol within Requirement 4 was 4.1.a [Implement and maintain a system and supporting processes to ensure that cardholder data is always encrypted during transit over unsecure networks], with 24.8% of organizations failing to pass muster.

The relatively high compliance with all these controls shows that these are common best practices. This has partly been driven by cardholders' increasing security awareness — many consumers now avoid websites that don't display the "green bar" or padlock indicating a secure connection.

No controls within Requirement 4 ranked in our "Top 20" or "Bottom 20" — though 4.1.1 came close, landing in twenty-first position.

Merchants performed slightly worse than service providers; our experience suggests that this is probably due to merchants continuing to use legacy systems that don't support strong encryption to transmit cardholder data.

This requirement is designed to protect cardholder data and sensitive authentication data transmitted over unprotected networks, such as the Internet, where it could be intercepted by attackers.

68.9%

OF COMPANIES MET ALL THE DEMANDS OF REQUIREMENT 4 IN 2013, AN INCREASE OF 34.9 PERCENTAGE POINTS ON 2012.

87.8%

IN 2013, COMPANIES WERE COMPLIANT WITH AN AVERAGE OF 87.8% OF CONTROLS.

Our 2013 DBIR dataset does not include a single security incident in which data was identified as being breached "in transit."

CLOUD COMPUTING

Companies of all kinds are increasingly adopting cloud computing services, and the merchants and service providers covered by PCI DSS are no exception. Cloud computing services offer many benefits, including increased agility and scalability, but as with any managed IT services, they alter the compliance landscape.

Providers can implement per-tenant, per-resource, and per-application security controls, keeping data secure despite the multi-tenant environment. Many on-premises environments rely on perimeter security as their only layer of defense and lack sufficient internal network access controls — so cloud environments can offer the same, or even better, security as their on-premises counterparts.

Organizations can protect transmitted card data in cloud environments in various ways; for example, ensuring that the cloud providers segment the deployment into public-facing and private segments, and maintain encryption (or re-encrypt if necessary) until card data reaches an application server in a secure, private segment of the cloud environment.

CHALLENGES AND PITFALLS

The biggest pitfall in complying with Requirement 4 is failing to understand the breadth of impact and the responsibilities it puts on the organization. For instance, should a customer email a merchant and include their card details in plain text, this could lead to unintended (and insecure) storage of cardholder data, and the merchant falling out of compliance with control 3.4.

Unsolicited emails

If a customer emails a merchant and includes their card details in plain text, the merchant must have a system in place to ensure that the PAN is either secured or securely deleted. Organizations receiving such messages should also respond to the sender advising them not to send card data by email. All organizations must regularly check for and securely remove any unsolicited card information that ends up in email servers and other databases.

Many organizations go one step further and use their DLP system's content filters to automatically block or quarantine any incoming or outgoing emails that contain cardholder data, helping ensure that the email system stays out of PCI-DSS scope. This may not be a practical solution for all organizations, and has potential downsides — like bringing the DLP systems and other components into scope.

Strong encryption

Requirement 4 covers any open, public networks or other messaging channels used to transmit unencrypted data — including email, efax, VoIP, instant messaging, customer support forums, and any other web session not protected by SSL/TLS. Unless organizations can find a way to adequately protect sensitive data passing through these channels, they may have to ban the use of these channels for sensitive data. The best practice is to extend the use of strong encryption widely across the organization, even beyond where cardholder data is usually transmitted.

The most commonly used method for the secure transmission of cardholder data is SSL/TLS. Most people are familiar with these cryptographic protocols from e-commerce, but they are also increasingly being used as the method of choice for point-to-point encryption (P2PE) solutions (see Appendix B, page 53). SSL/TLS can be used to satisfy the DSS requirement for network segmentation by isolating the transmission of cardholder data from the rest of the company's network traffic.

Devices between the endpoints of an encrypted communication are out of scope as long as they do not have the ability to decrypt the data.

If the organization being assessed has one of the endpoints in the SSL/TLS encryption, then the SSL/TLS process is in scope. To reduce the scope as much as possible, the organization can use terminals from the payment processor that encrypt data using keys created and held by the processor.

HOW IS THIS REQUIREMENT EVOLVING?

Efforts continue to address the security weaknesses currently inherent to wireless networking technologies on open public networks, such as weak legacy encryption and authentication protocols which allow attackers to exploit these vulnerabilities and gain privileged access to the CDE.

The phrase "open, public network" caused much confusion in the early days of PCI DSS. Control 4.1 was updated in both versions 2.0 and 3.0 of the standard to improve clarity, aligning the language used in describing testing procedures to that used in the requirement itself, and expanding the examples given.

Prior to 2013, lack of clarity caused uncertainty and concern around the requirements for protecting payment card data across cloud environments, in accordance with PCI DSS. In February 2013, the PCI SSC released the PCI DSS Cloud Computing Guidelines Information Supplement. This defines the security responsibilities of both the cloud provider and customer, and provides guidance for third-party cloud providers on how to secure payment data and maintain compliance with PCI-DSS controls in a cloud environment.

REQUIREMENT 5

Protect systems from malware and keep anti-virus software up to date

WHY IS IT IMPORTANT?

Attackers can use malware — malicious code — to gain a foothold in the environment, capture cardholder data, and damage systems; so it's important for organizations to protect all systems processing or storing CHD with anti-virus software.

Requirement 5 demands that anti-virus software is not only in place, but also that it is kept up to date; is capable of detecting, removing, and protecting against all known types of malware; generates audit logs; and that scans are performed regularly.

HOW DOES THIS REQUIREMENT RELATE TO SECURITY THREATS?

According to the 2013 DBIR, 40% of breaches involved malware, placing it the second-most common threat action. 74% of malware breaches involved direct installation on systems by attacker themselves, and 47% involved email attachments opened by legitimate users, like employees.

When our RISK team assessed organizations that suffered a security breach, they found just 34.9% compliance with Requirement 5. The average compliance across all organizations in our study was 56.4%. This suggests a correlation between having effective anti-virus software in place and reducing data breaches.

THE STATE OF COMPLIANCE

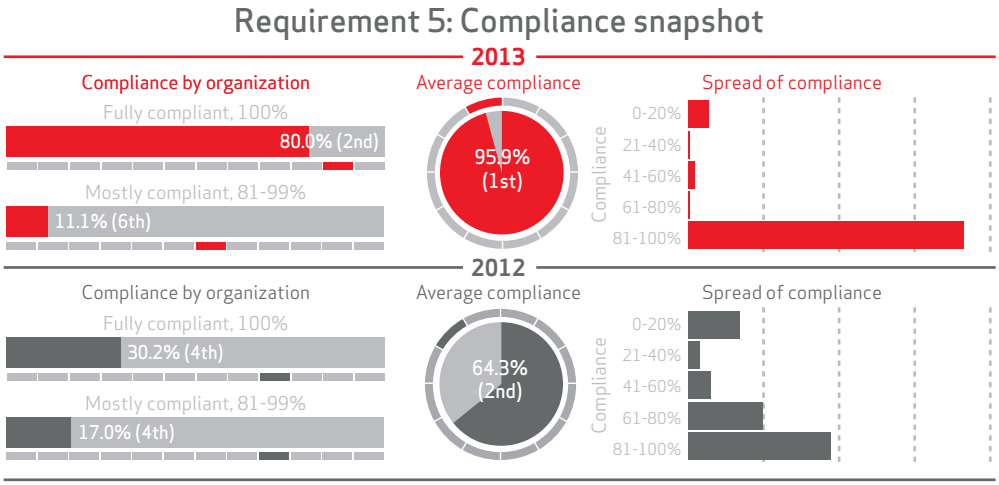


Figure 14: Snapshot for Requirement 5; dataset 2012 and 2013

In 2013, compliance leapt to 84.4% indicating that understanding of the requirement had matured or that anti-virus software and maintenance of services had improved. In order for an application to be compliant with PA-DSS, it must support virus scanning — so efforts to certify with PA-DSS are driving broader implementation of anti-virus/anti-malware protections.

Service providers proved significantly more compliant with this requirement than merchants.

We found that 86.1% organizations assessed on 5.1.1 [Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software] passed, putting it in our "Top 20".

Of all Requirement 5's controls and subcontrols, the one that organizations struggled the most with was 5.2.d [Ensure that anti-virus software log generation is enabled], with only 69.3% of assessments passed. A possible reason for this is that many large anti-virus suites provide their own logging capabilities, and these are often managed by a separate team.

This requirement concerns protecting all systems commonly affected by malicious software against viruses, worms, and trojans.

80.0%

OF COMPANIES MET ALL THE DEMANDS OF REQUIREMENT 5 IN 2013, AN INCREASE OF 49.8 PERCENTAGE POINTS ON 2012.

95.9%

IN 2013, COMPANIES WERE COMPLIANT WITH AN AVERAGE OF 95.9% OF CONTROLS.

SHAPE-SHIFTING

Modern malware is polymorphic, constantly changing to evade detection — like a spy slipping on a disguise. There have even been cases of malware being adapted to specifically target an individual organization. Signature-based technologies — like traditional anti-virus, anti-malware and intrusion detection systems — which work by matching characteristics of threats, do not provide adequate protection. Unfortunately, many companies — even large enterprises — still rely on these flawed technologies.

A study by Imperva in December 2012 found that "The initial detection rate of a newly created virus is less than 5%," and that "For certain antivirus vendors, it may take up to four weeks to detect a new virus from the time of the initial scan."[2]

Compliance with all other validation testing requirements exceeded 75%. This high level of compliance is probably because these controls cover some of the most basic security methods, and many organizations have a significant degree of process automation in place.

CHALLENGES AND PITFALLS

Historically, Requirement 5 has been associated with running local software that actively identified and blocked attacks. While there may have been some merit in creating and storing logs, organizations were often reluctant to place an additional performance overhead on systems. It's no coincidence, then, that when DSS 2.0 clarified that logging was a requirement, the greatest challenges with Requirement 5 revolved around logging and retaining logs.

Before DSS 3.0, any anti-virus software implemented in line with Requirement 5 did not explicitly address the newer threat of tailored malware, highlighted as a threat in the DBIR and similar studies. However, DSS 3.0 now redresses this balance by stating that organizations must be mindful of evolving malware:

The threat from malicious software can change quickly, so it is important that organizations keep abreast of current trends and developments. This can be achieved by monitoring security notices and news groups to determine what new and evolving malware threatens their systems and data.

HOW IS THIS REQUIREMENT EVOLVING?

There are only a few changes for DSS 3.0, though some are quite significant. Much of the language has been clarified to ensure that organizations know what is required. For example, the title was updated to reflect the intent of using anti-virus software: to protect systems against malware. And control 5.2 now aligns the language between requirement and testing procedures for consistency.

There is a new subcontrol and a new control within Requirement 5 in DSS 3.0:

- 5.1.2 requires organizations to regularly evaluate systems not considered to be a common target for malicious software. In the future, organizations must regularly evaluate evolving malware threats in order to confirm that such systems remain exempt from the requirement to have active anti-virus software. Historically, Linux's low share of the desktop market has meant that very little malware has been created for it (though that's changing), and led many to consider anti-virus software unnecessary. While rare on the desktop, around half of the world's webservers run on Linux and so this could have a significant impact.
- 5.3 strives to ensure that antivirus mechanisms are kept actively running. It states that users should not be able to disable or alter anti-virus/anti-malware software unless specifically authorized by management on a case-by-case basis; and if protection needs to be disabled for a specific purpose, it must be formally authorized and extra security measures should be implemented while it's inactive. Complying with this control will require strong policies, rigorous testing and monitoring, and fallback procedures to ensure continuity of protection.

REQUIREMENT 6

Develop and maintain secure systems and applications

WHY IS IT IMPORTANT?

Requirement 6 plays an important part in helping ensure that organizations maintain their security posture by:

- Managing and documenting changes in the CDE.
- Using secure development practices for applications in the CDE, whether developed internally or commissioned from third-party developers
- Ensuring that security policies are operational and documented
- Testing applications for the presence of known weaknesses and common design or coding flaws
- Identifying emerging vulnerabilities and remediating against them by applying software patches

Unless an organization knows what is in the environment at any point, it's impossible to assess risk accurately. DSS 3.0 makes it clear that change management applies across the board.

HOW DOES THIS REQUIREMENT RELATE TO SECURITY THREATS?

The 2013 DBIR showed that direct installation of malware on a compromised system was the most common attack vector. Stolen credentials and brute-force attacks were the most frequently observed ways of gaining access to systems. Requirement 6 specifies how organizations should harden their applications against attack; and compliance with this requirement therefore should help reduce vulnerability against this highly prevalent attack vector.

Investigations by our RISK team found that only 16.4% of organizations that had suffered a data breach were compliant with Requirement 6, compared to an average of 53.3% of all organizations assessed by our QSAs in 2013. This suggests a strong correlation between the likelihood of suffering a data breach and non-compliance with the PCI DSS.

THE STATE OF COMPLIANCE

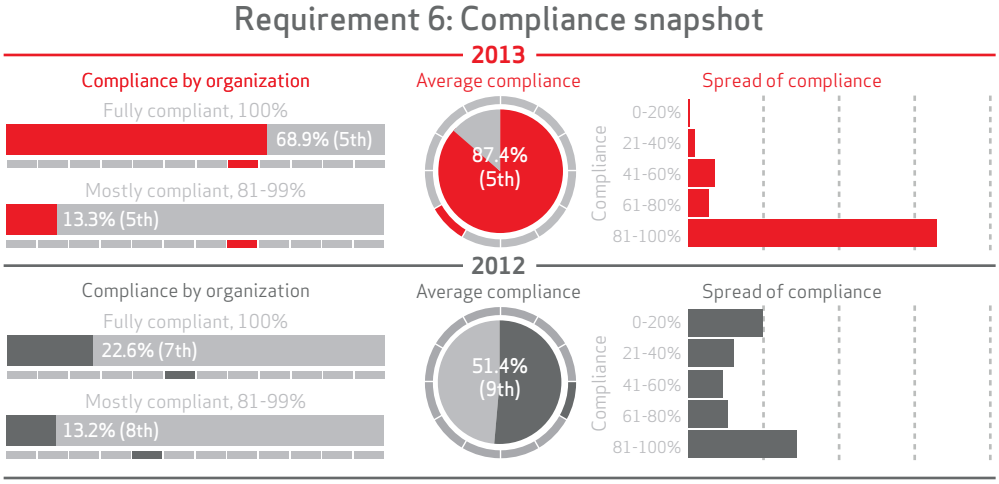


Figure 15: Snapshot for Requirement 6; dataset 2012 and 2013

Patch management can be a major headache for a large organization, that's why they often delay updates for as long as possible — many organizations skipped Windows Vista entirely, and 95% of the world's ATMs still run Windows XP. After June 30, 2012 the guidance within DSS control 6.2 specifying a risk ranking based on the Common Vulnerability Scoring System (CVSS) from the Forum of Incident Response Security Teams (FIRST) came into effect. This provides a "universal, open and standardized method for rating IT vulnerabilities," enabling companies to effectively prioritize the testing and deployment of patches. We believe that this contributed to the significant improvement in compliance with this requirement in 2013.

The three most-often complied-with subcontrols were all met by at least three-quarters of the organizations we analyzed. 6.5.b [Interview a sample of developers and obtain evidence that they are knowledgeable in secure coding techniques] is relatively simple to comply with, given the wealth of

This requirement covers how IT systems and applications, both in-house and third-party, are developed and maintained, whether by the organization or its suppliers. It recognizes that the threat landscape is always changing, and compliance measures need to change too.

68.9%

OF COMPANIES MET ALL THE DEMANDS OF REQUIREMENT 6 IN 2013, AN INCREASE OF 46.3 PERCENTAGE POINTS ON 2012.

87.4%

IN 2013, COMPANIES WERE COMPLIANT WITH AN AVERAGE OF 87.4% OF CONTROLS.

resources in secure coding available from major vendors such as Microsoft and Oracle. Subcontrols 6.4.4 and 6.3.1 govern the process of moving a system into production; specifying that test data, accounts and user IDs are removed before the system goes live — a one-off activity that's relatively easy to incorporate into launch processes.

The least-often complied-with subcontrols tended to be those related to the much more problematic areas of identifying and managing vulnerabilities and the associated changes on an ongoing basis. For example, 6.1.a (renumbered 6.2 in DSS 3.0) demands that systems and software are verified to have the latest vendor security patches installed. This subcontrol ranked among our "Bottom 20," with only 49.5% compliance.

CHALLENGES AND PITFALLS

Patch management

Patch management and associated vulnerability management processes represent the biggest problem areas, because they're rarely well documented and automated. Many weaknesses are only picked up during vulnerability scanning as part of Requirement 11.2, which means organizations are always playing catch-up.

The sheer scale of the task is also a problem. PCI DSS 3.0 states that all systems should have applicable vendor-supplied patches installed within an appropriate timescale according to prioritized risk, with critical patches installed within one month of release. Organizations must test patches for compatibility with systems and controls already in place before applying them to potentially thousands of devices, such as an estate of point-of-sale (POS) terminals across retail stores. As always, reducing the scope of the cardholder data environment should be the first step to reducing the patching workload.

The irony is that, as onerous as this patching requirement is, the effectiveness of Requirement 6 in terms of actually closing vulnerabilities depends largely on the responsiveness of third-party software and hardware vendors in releasing patches in the first place. An organization may be both compliant and still at risk if a vendor does not release a patch for a known vulnerability.

Organizations may find it challenging to maintain effective vulnerability management when an application or operating system reaches end-of-life and the vendor withdraws support. Relying on compensating controls to ensure effective data protection can only be a temporary solution, at best. Updating to a more recent release or alternative software offers a more robust and sustainable solution, and usually provides better ROI.

Change management

We also found significant problems with the change-management requirements covered under control 6.4, specifically relating to documentation and verification of changes. Change control is one of the key "gatekeeper" processes that maintain overall PCI-DSS compliance status. The cardholder environment is in constant flux, with new implementations and changes. The threat landscape also changes continually, with new attack vectors and vulnerabilities emerging.

However, to maintain the compliance status of the cardholder environment, the organization must ensure that system or business process changes do not impact or disable the current PCI-DSS controls, and that any new systems implement all required controls and integrate current security controls before going into production. These controls may include incident response, log monitoring and reporting, access control, patch management, and malware management, to name but a few. Change-management features, such as functionality testing and change impact assessment documentation, were not in place in about half of the organizations we assessed during 2011–2013. This means that organizations may be making changes that remove key controls already in place and lead to insecure implementation of systems within the CDE (as mentioned before, this includes connected systems).

Secure code development

Controls 6.3 and 6.5 govern secure code development, such as mandating code security reviews. Building security and compliance into the software development lifecycle requires a new set of skills; organizations need developers to:

- Be aware of common and emerging coding vulnerabilities (such as found in the OWASP 2013 Top 10 and SANS Top 20)
- Be able to identify and fix insecure code
- Document coding standards and best practices
- Follow testing procedures and checklists

These can all be a burden for an already overworked development team tasked with getting new functionality into production environments as quickly as possible.

The business must also change its behavior. When setting requirements for code development, business stakeholders should be aware that security testing must be passed before code enters a production environment. Even if the code passes functional tests, its implementation could still be delayed until security issues are addressed.

Cloud and web application firewalls

The emergence of the cloud has challenging implications for how organizations comply with control 6.6 in particular. This subcontrol is intended to ensure that externally facing web applications (including web services) stay protected against application-level attacks over time, either by reviewing or testing application code periodically or by deploying a web application firewall (WAF). When migrating applications to a cloud provider, it may no longer be possible for an organization to deploy a WAF in the provider's hosted environment, requiring the organization to re-evaluate how it will remain compliant with 6.6. This should be considered as part of any cloud migration strategy.

IN-MEMORY DATA

With customers expecting ever richer and responsive websites and applications, and IT striving to deliver real-time insight to the business, use of in-memory technology — like SAP HANA — is growing quickly. As ever, hackers have been quick to see what opening this offers, and we've seen an increase of malware that can sit resident on a system component and scrape data from memory.

Subcontrol 6.5.c is effective immediately. It requires that companies examine training records to verify that software developers received training on secure coding techniques. This means that application developers must demonstrate that they understand that the risks to sensitive authentication data (SAD) in memory and how it can be protected.

HOW IS THIS REQUIREMENT EVOLVING?

Requirement 6 was updated significantly in DSS 2.0 and again with the release of version 3.0. The overall wording of the requirement changed to specify that all applicable systems, not just critical ones, must have all appropriate patches applied, significantly increasing the scope of effort for organizations.

The updates include six new "best practices" that will become requirements on July 1, 2015, and over a dozen clarifications on existing controls. The changes covered:

- Securing authentication and session management in web applications. The new subcontrol 6.5.10 sets standards for web development practices, session control and timeouts, and testing of web applications that handle card data to reduce the probability of "man-in-the-middle" and client-side attacks.
- Following the regularly updated lists of vulnerabilities provided by, NIST, OWASP, SANS, and CERT — vulnerability management must be made part of business as usual.
- Clarifying that change management applies to all changes to all system components, not only during software development and maintenance.
- The secure handling of cardholder data in memory, reflecting the increasing number of attacks targeting data at the time of processing.

This requirement specifies the processes and systems that restrict each user's access rights to the minimum they need to perform their duties — in other words, "need to know."

73.3%

OF COMPANIES MET ALL THE DEMANDS OF REQUIREMENT 7 IN 2013, AN INCREASE OF 31.8 PERCENTAGE POINTS ON 2012.

86.8%

IN 2013, COMPANIES WERE COMPLIANT WITH AN AVERAGE OF 86.8% OF CONTROLS.

The attackers may be external, or they may be insiders acting maliciously (or carelessly). In either case, restricting each user account's privileges is an important part of preventing damage being caused.

REQUIREMENT 7

Restrict access to cardholder data by business need to know

WHY IS IT IMPORTANT?

Every user account with access to cardholder data (and the systems that store it) is a potential security risk. The more people granted access to sensitive data, the bigger the target you offer to attackers, and the greater the risk of accidental or deliberate misuse by staff. Complying with this requirement is key to ensuring that critical data can only be accessed by personnel who need it to perform their roles.

Requirement 7 covers policies and controls for both physical and IT security. An access-control system for each element of the cardholder data infrastructure must be in place, including using locks or restricted access to paper-based cardholder data records or system hardware; controlling access to the wireless network, PCs, and other devices; and controlling access to any digital files that contain cardholder data.

Access controls should be limited on the basis of "need to know" or "least privilege," giving each individual the minimum privileges and access to data required to perform their role.

In order to ensure consistency and deal with changes caused by recruitment and employee termination, it is essential that access management is automated, based on well-defined roles, and enforced across all components of the CDE and connected systems. Roles themselves should be structured to ensure separation of duties.

HOW DOES THIS REQUIREMENT RELATE TO SECURITY THREATS?

The DBIR makes it clear that abuse of user privileges is a favored channel for attackers trying to capture data. Gaining access via a genuine, authorized account — by guesswork (brute force/cracking) and/or phishing (increasingly including social engineering) — is often the most direct way to gain illegitimate access to a system, and one of the hardest to detect. The DBIR found that more than half of all breaches involved hacking, and that authentication-based attacks factored into about four of every five of these breaches. Furthermore, 66% of exfiltrated data was taken from databases and file servers, and commonly accessed through legitimate (but misused) credentials.

There's also a real risk from users themselves. 14% of attacks that we investigated in the 2013 DBIR involved "insiders" — legitimate users with access rights to company systems. Customer service personnel were responsible for 46%, end-users 33%, managers 7%, and executives 5%. These groups are not system administrators nor are they IT security experts, and they generally do not need extensive access privileges.

Our DBIR-related investigations found that only 31% of organizations that suffered a breach were compliant with Requirement 7, compared to an average of 74% of all organizations assessed by our QSAs. This suggests a strong correlation between the likelihood of suffering a data breach and a lack of compliance with PCI DSS.

THE STATE OF COMPLIANCE

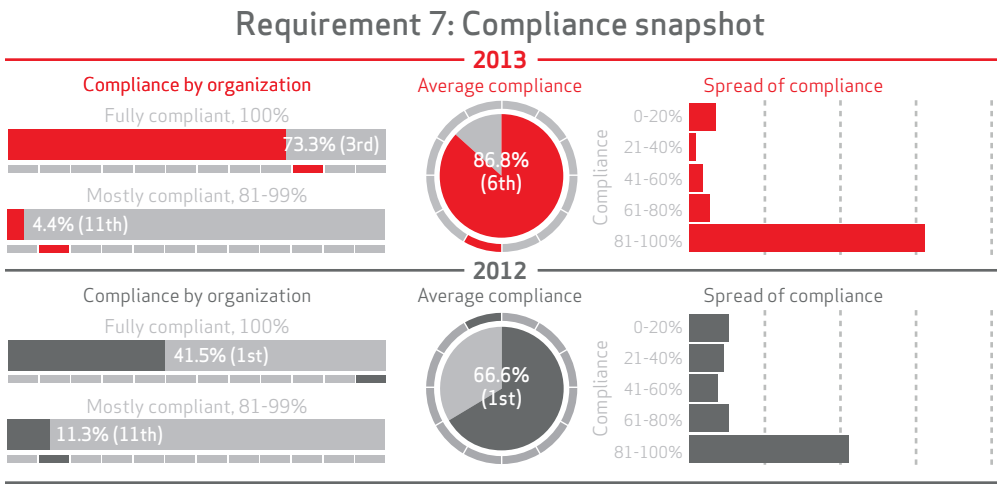


Figure 16: Snapshot for Requirement 7; dataset 2012 and 2013

The subcontrols most-often complied with cover technical considerations: the implementation of automated access-control systems (7.1.4) to cover all system components (7.2.1), with "deny all" set by default (7.2.3). More than 80% of organizations were compliant with each of these subcontrols.

The subcontrols least-often complied with showed that organizations are struggling with role-based access controls and defining least privilege:

- Only 73.3% of organizations met control 7.1.2, which requires that privileges are assigned to individuals based on job classification and function.
- Just 68.3% of companies complied with 7.1.1, which requires that access rights for privileged user IDs are restricted to the least privileges necessary to perform job responsibilities.
- A mere 65.3% of companies were compliant with 7.2.2, which requires that access-control systems are configured to enforce privileges assigned to individuals based on job classification and function.

CHALLENGES AND PITFALLS

Although most organizations don't appear to struggle with Requirement 7, there is certainly room for improvement in increasing the understanding of how its controls can be implemented more effectively.

Organizations must realize that it's not acceptable to allow any privileged user to have access to all data. Permissions should be granted based upon the specific role and responsibility, which must be tied directly to the applications and processes a user requires access to in order to perform their defined role.

Defining the user roles and appropriately constructing the privileges and the controls that restrict access at a conceptual level is the core task. This is challenging enough, but the organization then needs to translate a set of privileges into system configurations implemented across the infrastructure. Access controls may be governed simultaneously in individual applications, databases, and at the operating system level.

HOW IS THIS REQUIREMENT EVOLVING?

Requirement 7 has remained fairly static since the release of DSS 1.2.1 — when DSS 2.0 was released, it clarified just two security controls. But this requirement received more attention with the release of DSS 3.0:

- 7.1.1 was added to cover the definition of access needs for each user role, an important foundational step.
- 7.1.2 refocused the requirement on restriction of privileged user IDs to least privileges necessary, and enhanced testing procedures.
- 7.1.3 refocused on assignment of access based on an individual's job classification and function attacks targeting data at the time of processing.

"Deny by default" means that users must be explicitly assigned to a whitelist to access networks and applications, making access control both more effective and simpler to manage.

Organizations must realize that it's not acceptable to allow any privileged user to have access to all data.

This requirement sets standards for managing user identities and authentication methods, including passwords. Until DSS 3.0, it was called "Assign a unique ID to each person with computer access."

62.2%

OF COMPANIES MET ALL THE DEMANDS OF REQUIREMENT 8 IN 2013, AN INCREASE OF 39.6 PERCENTAGE POINTS ON 2012.

84.1%

IN 2013, COMPANIES WERE COMPLIANT WITH AN AVERAGE OF 84.1% OF CONTROLS.

Regardless of the authentication mechanism(s) used, credentials must be linked to an individual account and only provide a single user with access.

REQUIREMENT 8

Identify and authenticate access to system components

WHY IS IT IMPORTANT?

Assigning individual user identities is a vital part of ensuring that only the right people have access to sensitive data and systems, and that a clear audit trail can be established. Shared accounts make it very difficult to restrict and monitor access to individuals by "need to know". Organizations need accountability: only when each individual has a uniquely identifiable account can the organization determine exactly who has been accessing systems and data — the first step in tracing how a breach happened.

Authentication credentials, particularly passwords, are a prime target for attackers. Passwords can be lost or stolen, and weak ones can be cracked easily using brute-force methods. This requirement sets standards for password strength, covers use of other authentication credentials such as two-factor authentication (particularly for remote access), and helps protect systems against password cracking attempts (e.g. by limiting login attempts). It also governs how user credentials are protected at the time of use, during transmission, and in storage.

HOW DOES THIS REQUIREMENT RELATE TO SECURITY THREATS?

Our DBIR makes a clear case for the importance of effective authentication to system security. 76% of all network intrusions exploit weak or stolen credentials. And in many cases these are very simple attacks using readily available password cracking tools. Organizations can close such vulnerabilities with straightforward measures; DBIR analysis suggests that simply using something other than single-factor username/password credentials would have likely thwarted 80% of the hacking attacks we investigated.

The 2013 DBIR also reports that "more than half of insiders committing IT sabotage were former employees who regained access via backdoors or corporate accounts that were never disabled." Requirement 8 helps close this hole by demanding that accounts of former employees be disabled and removed promptly. Strict policies and good coordination between supervisors, human resources, and the network operations team is necessary.

According to our RISK team's assessments, only 24.2% of organizations that suffered a security breach were compliant with Requirement 8 at the time of their breach.

THE STATE OF COMPLIANCE

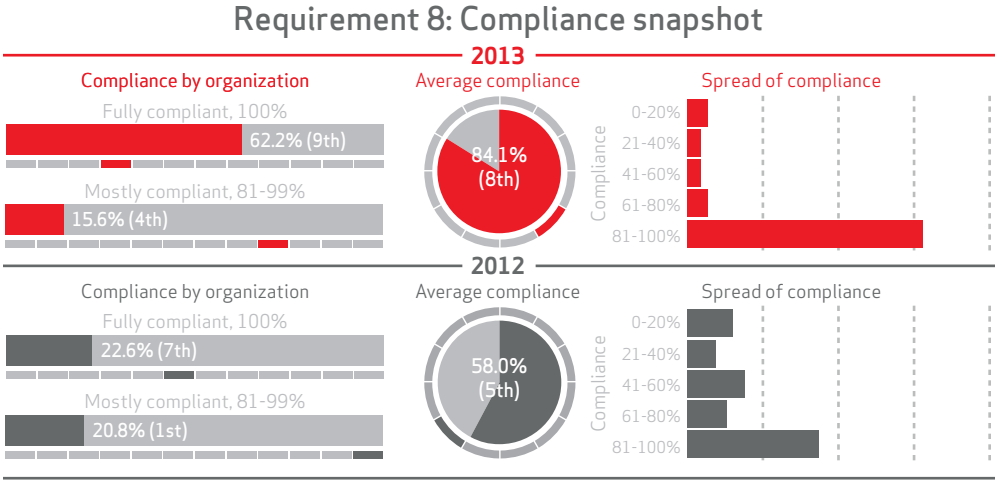


Figure 17: Snapshot for Requirement 8; dataset 2012 and 2013

The large increase between 2012 and 2013 can be partly explained by better understanding of two-factor authentication. Not only have the tools available to security administrators improved, but users have also become more familiar with strong authentication techniques — online services from banking to Gmail brought them into peoples' everyday lives.

We found a massive variation in compliance with particular subcontrols. Seven of the subcontrols in Requirement 8 (8.5.10.b, 8.5.12.b, 8.5.13.b, 8.5.9.b, 8.4.b, 8.5.11.b, 8.5.7) are in our "Top 20" — in fact all seven are in the top 10, each with over 90% compliance. But Requirement 8 also had one subcontrol in our "Bottom 20" — only 57.4% of organizations complied with 8.5.1, which governs the addition, deletion, and modification of IDs and credentials.

Organizations also had problems complying with some important subcontrols that have a clear link to protecting against common attacks. For example, only 62.4% of organizations complied with 8.5.15, which specifies that idle sessions expire after no more than 15 minutes. Hijacking sessions is a popular way for attackers to get in to applications. And the same percentage complied with 8.5.13.a, which requires that users are locked out after no more than six failed login attempts. Again, this is a simple way to make sure that brute-force (password guessing) attacks are blocked. In case you're left wondering, no, it wasn't always the same companies; 55.4% complied with both, 13.9% with just one, and 30.7% with neither.

Authentication credentials, particularly passwords, are a prime target for attackers. Passwords can be lost or stolen, and weak ones can be cracked easily using brute-force methods.

CHALLENGES AND PITFALLS

Requirement 8 doesn't apply to users such as cashiers, who only have access to one cardholder record at a time; it's intended for workers in offices and datacenters who have specific access to databases and other systems in the cardholder data environment. These kinds of users are often already familiar with password policies, so organizations have few major stumbling blocks to compliance.

The challenges tend to be smaller, operational and often in areas that organizations wouldn't think to look. For instance, many system and database administrators require temporary privileged access to systems as part of their work. Directly accessing a shared root or admin account; for example through "su" (substitute user or superuser) isn't permitted under Requirement 8, which specifies that each user must have a unique ID. However, it may be possible to perform these tasks using other commands (e.g., "sudo") that log the actions performed to a specific individual and their personal credentials.

Legacy applications also pose a challenge. Coding for session timeouts and maximum login attempts is trivial, but adapting legacy systems to meet these standards isn't always easy.

HOW IS THIS REQUIREMENT EVOLVING?

This requirement changed significantly in DSS 2.0 and again in DSS 3.0. Most noticeably, it was renamed to better reflect the full scope of identification and authentication management.

The changes to the Requirement 8 controls in DSS version 3.0 align issues between control requirement and validation testing procedure. They provide much of the needed flexibility in authentication, and broaden the requirement to cover a wider range of scenarios to reflect the modern view that passwords are often an inadequate way of authenticating secure access. This will benefit organizations that have already moved, or are considering moving away from merely using passwords for authentication. Changes include:

- References to passwords have been changed to "authentication credentials" throughout the text
- The minimum password complexity and strength requirements have been combined into subcontrol 8.2.3, increasing the flexibility to use alternatives
- Control 8.6 now includes consideration for other authentication mechanisms, such as certificates, physical security tokens, and smart cards

Other changes to Requirement 8 include:

- Identification and authentication have been split into separate controls
- Management of "processes" to ensure machine-to-machine (M2M) access is properly authorized was added
- Subcontrol 8.5.1, a best practice until July 1, 2015, will require service providers with remote access to customer environments to use unique authentication credentials for each customer

Simply using something other than single-factor username/password credentials would have likely thwarted 80% of the hacking attacks we investigated.

This requirement requires organizations to lock down physical access to systems that store, process, or transmit cardholder data.

86.7%

OF COMPANIES MET ALL THE DEMANDS OF REQUIREMENT 9 IN 2013, AN INCREASE OF 50.9 PERCENTAGE POINTS ON 2012.

94.9%

IN 2013, COMPANIES WERE COMPLIANT WITH AN AVERAGE OF 94.9% OF CONTROLS.

REQUIREMENT 9

Restrict physical access to cardholder data

WHY IS IT IMPORTANT?

For organizations focusing on preventing hacking, viruses, and other types of electronic data breaches, physical breaches are easy to overlook. Without appropriate physical security in place, attackers — including rogue staff — can remove or copy cardholder data by tampering with POS devices, stealing receipts, or many other methods.

Requirement 9's controls demand that organizations use secure entry controls to prevent unauthorized physical access to systems in the cardholder data environment. It also states that organizations must secure media that carries cardholder data, restrict sharing, limit the retention of cardholder data, and protect POS devices against tampering.

HOW DOES THIS REQUIREMENT RELATE TO SECURITY THREATS?

According to the 2013 DBIR, 35% of breaches involved physical attacks. Of those, tampering accounted for 91% of attacks — and ATMs and POS devices were the two most commonly compromised assets. The physical security controls set out in Requirement 9 restrict access to cardholder data, making it harder for attackers to conduct physical attacks successfully. Limiting retention of data would also lessen the damage caused by a successful physical attack.

THE STATE OF COMPLIANCE

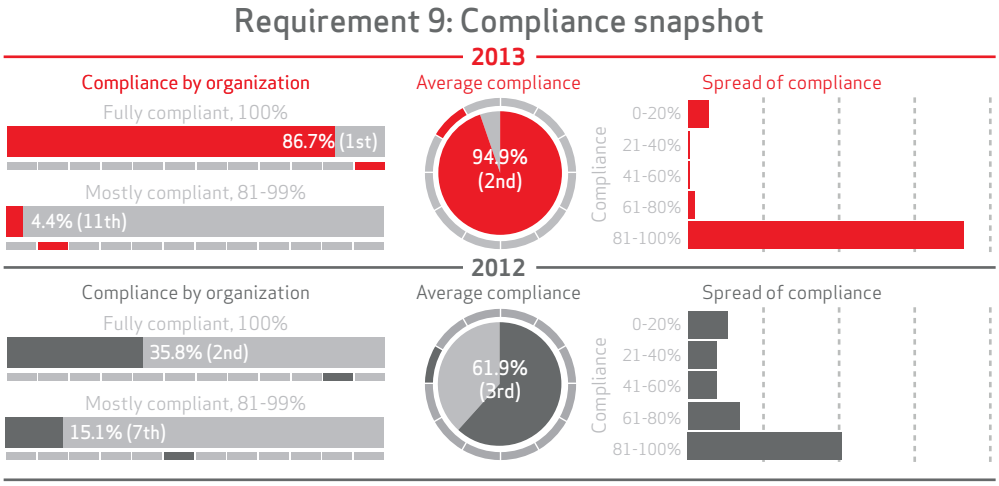


Figure 18: Snapshot for Requirement 9; dataset 2012 and 2013

Five of Requirement 9's subcontrols (9.1.3, 9.1.2, 9.3.3, 9.3.1 and 9.3.2.b) make it into our "Top 20." These refer to restricting physical access to network hardware, and making sure all visitors are authorized (with specific controls before entering areas where CHD is processed or maintained). These achieve between 86.1% and 91.1% compliance, showing that organizations are generally pretty strong on controlling physical access.

Just 66.3% of organizations were compliant with 9.9.1 [Properly maintain inventory logs of all media and conduct media inventories at least annually]. This low level of compliance could be because organizations see logging as a resource-intensive task that adds little value — we disagree — and organizations that do maintain logs may forget about backups or USB devices containing CHD.

But surprisingly, 74.3% of organizations were compliant with 9.8 [Destroy media when it is no longer needed for business or legal reasons].

CHALLENGES AND PITFALLS

With server virtualization now commonplace in enterprise environments, many organizations find it difficult to identify and track which servers run which tasks. The applications and data that run on a specific physical enclosure can, and will, change frequently. This can have huge implications for your organization's ability to define what is in scope for compliance and to conduct effective logging and documentation.

For effective access control, organizations should relate Requirement 9 closely with Requirement 7, which addresses key principles of access control, and Requirement 8, which addresses technical and logical access control for information systems. Organizations should coordinate logging and documentation closely across these three requirements, so they can easily identify what has happened at any point by comparing logs and documents.

TRUE STORY: AS SEEN ON TV

While assessing an acquirer, one of our QSAs noticed that their network operations center's large wall displays were visible from of one the building's public areas — and that they had card data scrolling on a web supervisor log screen. The room had wireless routers clearly visible, and the Wi-Fi was completely unprotected. All our QSA had to do was type in the URL visible on the displays to get access to the log of card numbers. Further investigation showed that we could also access and query the acquirer's database which held millions of entries.

HOW IS THIS REQUIREMENT EVOLVING?

DSS 3.0 has introduced two additional controls, clarified the existing language, and reorganized the subcontrol numbering to help organizations understand what is required of them.

One of the additions (control 9.3) demands that organizations control physical access to sensitive areas for onsite personnel. Only authenticated access based on individual job function is permitted — and access must be revoked immediately when that person leaves the organization or changes role. This subcontrol works in conjunction with Requirement 7, which states that organizations must limit critical data to authorized personnel on a "need-to-know" basis.

The other addition (control 9.9) addresses the rise of physical attacks on POS devices. It was always the intention that this requirement covered POS terminals, but DSS 3.0 makes it explicit. Organizations must protect any device that has direct interaction with a card against tampering and substitution to help prevent "skimming" and data interception attacks. Control 9.9 also states that organizations must hold an inventory of systems, inspect POS devices, and provide employee training. This control includes some flexibility — it only requires "periodic" inspection of devices to look for tampering or substitution — but it is still perceived to be difficult to implement in large environments.

It's just considered a "best practice" for now, but from July 1, 2015 adherence will be required to achieve compliance. While it's good to see this added to DSS 3.0, many acquirers already place strict requirements on the control of payment devices as part of their contract with merchants — these are often more exacting than this control.

This requirement covers the creation and protection of information that can be used for tracking and monitoring of access to all systems that store, process, or transmit cardholder data, including databases, network switches, firewalls, and clients.

60.0%

OF COMPANIES MET ALL THE DEMANDS OF REQUIREMENT 10 IN 2013, AN INCREASE OF 39.2 PERCENTAGE POINTS ON 2012.

82.2%

IN 2013, COMPANIES WERE COMPLIANT WITH AN AVERAGE OF 82.2% OF CONTROLS.

REQUIREMENT 10

Track and monitor all access to network resources and cardholder data

WHY IS IT IMPORTANT?

Organizations must be able to track how users (legitimate or otherwise) are accessing resources if they're to detect and prevent potential data compromises.

The main mechanism for achieving this tracking and monitoring is to use system activity logs. Most applications, network appliances, and software packages can perform the level of logging required for PCI-DSS compliance. Logs also enable organizations to analyze and determine the cause of a compromise during investigations after a breach.

Consistent and complete audit trails can also significantly reduce the cost of a breach. A large part of post-compromise cost is related to the number of cards thought to be exposed. Lack of conclusive log information reduces the forensic investigator's ability to determine whether the card data in the environment was exposed only partially or in full. Because the issuers usually pass on the full costs incurred in reissuing cards to the breached organization, knowing precisely which cards were actually exposed directly influences the financial impact.

Requirement 10's various controls are designed to ensure that logs are monitored for proactive detection of issues, and archived in a secure manner to allow for use in forensic investigations.

HOW DOES THIS REQUIREMENT RELATE TO SECURITY THREATS?

Organizations can't prevent or address a breach unless they can detect it. Active monitoring of the logs from their cardholder data environments enables organizations to spot and respond to suspected data breaches much more quickly.

Our data shows that most organizations that suffered a data breach lacked effective log management. Only 9.4% of organizations that our RISK team investigated after a data breach was reported were compliant with Requirement 10. By comparison, our QSAs found 31.7% compliance with Requirement 10. This suggests a correlation between the lack of effective log management and the likelihood of suffering a security breach.

Only 9.4% of organizations that our RISK team investigated after a data breach was reported were compliant with Requirement 10.

It's important to note that many of the organizations that were assessed as being non-compliant at the time of their breach had successfully complied during their previous PCI-DSS assessment, indicating that these organizations had failed to embed continuous compliance practices as part of "business as usual" and had instead lapsed back into non-compliance.

TRUE STORY: GOING ROGUE

During a PCI-DSS assessment at a large European company, one of the IT directors assured our QSAs that the company's CDE had absolutely no wireless access points. But during inspection of the main facility, the QSAs noticed a strong wireless signal coming from a rack in the data center. Upon opening the rack, they discovered an access point connected directly to the server hosting the cardholder database. It turned out that an administrator had installed the access point some months earlier so that he could access the database from a more comfortable office elsewhere in the building. This highlights an important fact: the wireless elements of the DSS are as much about actually looking for rogue access points as they are about checking the security of known wireless infrastructure.

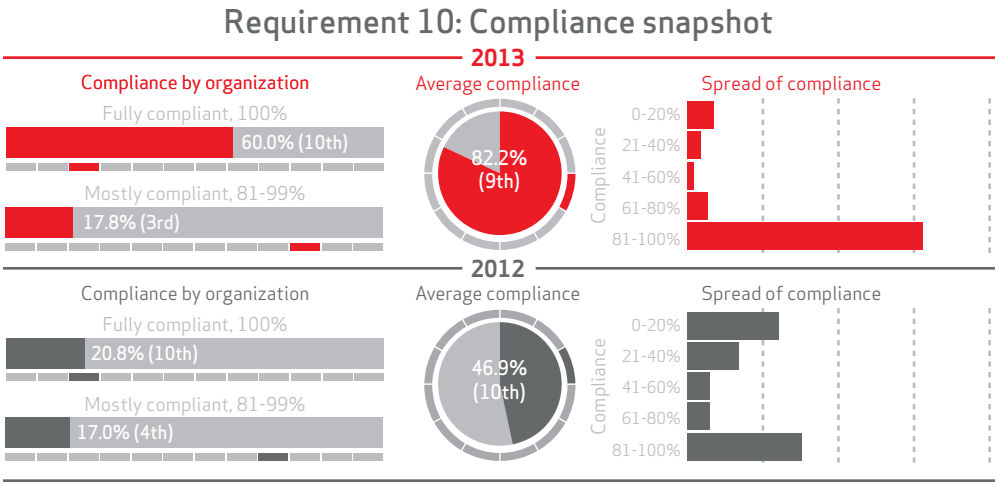


Figure 19: Snapshot for Requirement 10; dataset 2012 and 2013

Organizations generally find enterprise log management hard, in terms of generating logs (covered in controls 10.1 and 10.2), protecting them (10.5), reviewing them (10.6), and archiving them (10.7). Furthermore, many of the controls within Requirement 10 are interdependent, and failing to comply with one can have a knock-on effect on compliance with several others.

But the trends are promising: in 2013 the average rose to 82.2% and 60.0% of organizations were fully compliant. The year-on-year trends are consistent with results for other requirements: a drop as DSS 2.0 was introduced in 2011, bringing many changes and clarifications versus DSS 1.2.1; a further fall as PCI Security testing requirements became more stringent in 2012; and a significant increase by 2013 as organizations became more mature in their compliance practices.

During the past three years, the challenges around Requirement 10 received a fair amount of attention in the industry, which heightened corporate awareness around the need to address logging and monitoring using a combination of suitable tools (such as security information and event management (SIEM) systems) and having the business processes in place to support those tools.

One of the most challenging parts of Requirement 10 appears to be control 10.4. This specifies that access to time data is restricted, external time signals are properly used, and that changes to time settings are logged, monitored, and reviewed. We found that just 49.5% of organizations were compliant with all parts of this control between 2011 and 2013.

While using network time protocol (NTP) to synchronize time across systems is commonplace, control 10.4 specifies a particular deployment of NTP to address exploitable system vulnerabilities. It requires that only designated central time servers receive time signals from external sources, so you need trusted time sources on the outside and all other internal servers to synchronize with your designated internal time servers. The central time servers that need to make outbound external connections must be in the demilitarized zone (DMZ), with a firewall allowing communication (to meet subcontrol 1.3.3). Authentication can be added so that each client can be sure it's speaking to designated time servers, and not directed to a rogue server due to a DNS poisoning attack.

Time data is critically important to using logs effectively, so we expect the DSS to continue to emphasize this aspect of Requirement 10.

Two subcontrols within Requirement 10 appear in our "Bottom 20":

- 10.4.1.a [Verify that only designated central timeservers receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC], (55.4%)
- 10.4.2.a [Review system configurations and time-synchronization settings to verify that access to time data is restricted to only personnel with a business need to access time data], (55.4%)

49.5%

OF COMPANIES WERE COMPLIANT WITH CONTROL 10.4. THIS SPECIFIES A PARTICULAR DEPLOYMENT OF NTP TO ADDRESS EXPLOITABLE SYSTEM VULNERABILITIES.

THE KEY TO DETECTING BREACHES EARLY

Aware that traditional methods of identifying attacks are no longer sufficient, the IT security industry has developed a new approach based on indicators of compromise (IOCs). RSA, the security division of EMC, defines an IOC as "a forensic artifact or remnant of an intrusion that can be identified on a host or network." IOCs include traditional signs of an attack, like unusual traffic (for example an unusual volume for the time of day); checksums and changes in firewall configurations; and more advanced signs that are much harder for attackers to hide, like memory artifacts. IOCs enable companies to be more proactive in identifying attacks, and help spot more sophisticated attacks by considering multiple signs together. While it's not an explicit requirement of PCI-DSS compliance, we recommend that you look at IOCs as a way to improve your defenses.

66%

OF THE BREACHES IN OUR 2013 DBIR TOOK MONTHS OR EVEN YEARS TO DISCOVER.

Verizon 2013 DBIR

CHALLENGES AND PITFALLS

Log management impacts business processes, information technology systems, third-party organizations, and in many instances is required to go well beyond the scope of data protection for PCI Security compliance. Organizations that achieve log management success realize the benefits of approaching Requirement 10 as a broader business issue, and as an opportunity to improve overall data protection and information security across the business — beyond merely an investment for PCI Security compliance purposes.

Achieving log management success requires careful planning, a sound strategy, and ongoing management with continuous improvement. Standards such as NIST Special Publication 800-92 define how to implement good log management practices.

Requirement 10 was never meant to be solely about using system logs to detect data breaches — implementing effective log management has numerous other operational benefits. Organizations that implement a central log server focusing on this as the sole objective often fail to design and implement a sustainable log management solution.

Organizations must realize that it is impossible to effectively review log files manually, regardless of the number of system components in any particular cardholder data environment.

Importantly, organizations must realize that it is impossible to review log files manually with the required effectiveness, regardless of the number of system components in any particular cardholder data environment, be it one server or one hundred. The task must be automated to generate exception reports and alerts. And automation tools must be appropriately configured to avoid overwhelming smaller security teams with data, particularly when it comes to daily reviews. Even the best event alerting will fail to provide appropriate protection if security procedures aren't established to coordinate a quick and appropriate response to events.

By analyzing a large number of attacks, it's possible to create lists of signs that a breach may have happened, or be about to. In the quest to detect data breaches more quickly, these IOCs can provide vital early warning. Typical IOCs include anomalies in traffic patterns, unusual patterns of requests (perhaps indicating a script rather than a human at work), and activity from strange places and at strange times. Incorporating IOC intelligence into your security regime can help you spot malicious activity on systems more quickly, preventing a breach from happening or at least stopping it in its early stages.

HOW IS THIS REQUIREMENT EVOLVING?

The changes to Requirement 10 in version 3.0 of the DSS include clarifying the meaning of certain controls. For instance, the section on daily log reviews was revised to help organizations focus their log-review efforts on identifying suspicious activity, relaxing the need to review of logs deemed to be less critical (according to the organization's risk management strategy). However, the new standard now also specifically mentions the need to detect anomalies so some current processes and policies may need to be reviewed for compliance with DSS 3.0.

There were also two changes that evolved the requirement. Subcontrol 10.2.5 covers logging use of and changes to identification and authentication mechanisms, including changes to administrator accounts. This is intended to help verify which accounts were involved in a given incident and block attacks impersonating valid accounts. Subcontrol 10.2.6 was updated to prevent the stopping or pausing of audit logs, a common practice for malicious users trying to avoid detection.

REQUIREMENT 11

Regularly test security systems and processes

WHY IS IT IMPORTANT?

There has been a significant change in attitude toward Requirement 11 over the years. In early versions of the DSS this was perhaps seen as a number of "testing activities" that needed to be performed by an external specialist organization, almost as a final check on the controls. This testing is now clearly an integral part of the validation process for many of the other requirements; and a mandatory part of how organizations validate their compliance scope (DSS 3.0 control 11.3).

HOW DOES THIS REQUIREMENT RELATE TO SECURITY THREATS?

Requirement 11 demands that organizations have a sustainable network and application vulnerability management program, and that they evaluate the overall effectiveness of security measures in place across the organization. As a result, it's fundamental to ensure that the organization is prepared against the range of attack types reported in the DBIR. Our data shows that most organizations that suffered a breach weren't compliant with Requirement 11. During post-breach investigations, our RISK team found that just 13.2% of organizations were compliant with this requirement.

Requirement 11 tests the security posture and the effectiveness of other PCI Security controls.

THE STATE OF COMPLIANCE

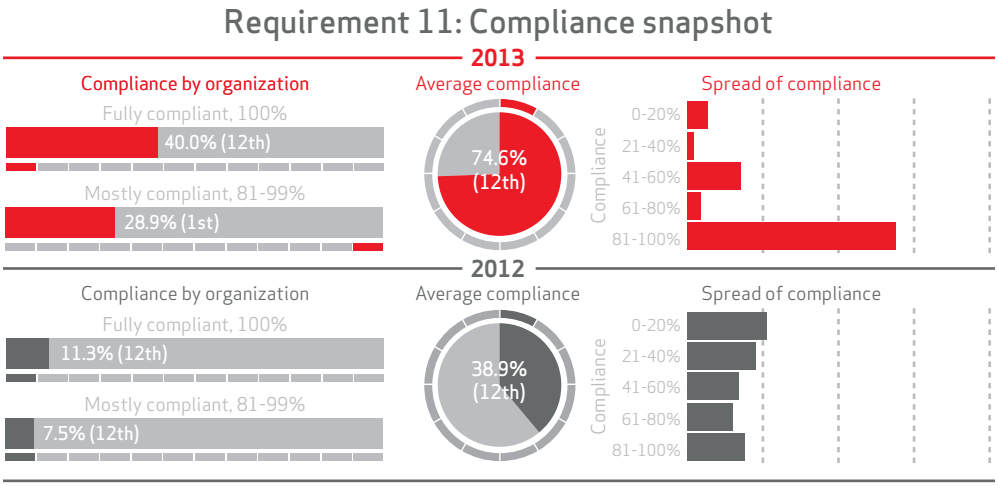


Figure 20: Snapshot for Requirement 11; dataset 2012 and 2013

Requirement 11 was the least complied-with requirement in our study. Just 23.8% of companies met all the controls between 2011 and 2013. But when we look at the data year-by-year, we can see an improvement. In 2012, a mere 11.3% of companies complied (and the average compliance was just 38.9%). In 2013 this rose to 40.0% (and the average leapt to 74.6%), though it languished in the bottom slot both years.

The Requirement 11 controls and subcontrols where we saw the lowest compliance between 2011 and 2013 were:

- 11.3.a [Examine the results from the most recent penetration test to verify that penetration testing is performed at least annually], 39.6%
- 11.3.b [Verify that noted exploitable vulnerabilities were corrected and testing repeated], 43.6%
- 11.2.1.a [Review the scan reports and verify that four quarterly internal scans were performed in the most recent 12-month period], 45.5%

This requirement covers the regular vulnerability scanning and penetration testing of processes, applications, and networks to be performed by the organization itself, and/or an independent third party on its behalf.

40.0%

OF COMPANIES MET ALL THE DEMANDS OF REQUIREMENT 11 IN 2013, AN INCREASE OF 28.7 PERCENTAGE POINTS ON 2012.

74.6%

IN 2013, COMPANIES WERE COMPLIANT WITH AN AVERAGE OF 74.6% OF CONTROLS.

"A vulnerability scan (or even a vulnerability assessment) looks for known vulnerabilities in a system and reports potential exposures. A penetration test is designed to actually exploit weaknesses in the system architecture or computing environment. Where a vulnerability scan can be automated, a penetration test requires various levels of tester expertise."

Berkeley Security, University of California[3]

CHALLENGES AND PITFALLS

Use of third parties

As is evident from our "Bottom 20" list, many organizations have a problem with needing to work with external organizations throughout the year on vulnerability and penetration testing scans. Most of the controls that involve recurrent use of third parties, Approved Scanning Vendors (ASVs) scans are excluded as they can be launched internally, have a low compliance percentage — in fact, Requirement 11 dominates our "Bottom 20" list, taking 11 places (including the six very lowest).

Misunderstanding the purpose of vulnerability scanning

This Requirement is still proving troublesome for some, even though the PCI SSC has given organizations some leeway: control 11.2 permits organizations working to become compliant for the very first time to present only the last quarterly vulnerability scan — instead of the four normally required.

Vulnerabilities should be identified as part of a broader vulnerability management process, using reputable outside sources of information. Once identified, classified, and corrected, network and application vulnerability scans serve as an important check to verify a component or environment no longer contains vulnerabilities — within the limitations of current scanning methods.

Neglecting penetration testing

Our data shows that many organizations fail to comply with penetration-testing controls. This is partly due to the requirement that tests are to be run against the final infrastructure — so testing is often conducted at the last minute, just before a compliance validation assessment.

Often our QSAs are given a penetration-testing report only to find that the organization hasn't even read it.

This is not the only problem. The penetration-testing market is becoming increasingly price-driven, with many low-quality services emerging. Some of these may not thoroughly test the environment and may miss more difficult attack vectors — meaning that vulnerabilities are missed, but the organization still gets a pass.

Organizations that are looking simply to comply are incentivized to opt for the cheapest, quickest and most superficial testing that will allow them to "check the box".

Many organizations also struggle to conduct penetration testing with the required frequency, both internal testing and when purchasing a new test after "any significant change." The cost and workload no doubt deter many; and indeed without a robust methodology in place for conducting risk assessments, it can be challenging to identify what counts as a "significant change" in the first place.

Wireless environments

Organizations performed adequately on subcontrol 11.1.a, which requires organizations to verify that the entity has a documented process to detect and identify wireless access points on a quarterly basis, with 67.3% compliant — it's the fifth-most commonly in-place control within Requirement 11. But wireless remains a real issue: some of the largest data breaches in history occurred as result of insecure and unknown (or "rogue") wireless access points.

HOW IS THIS REQUIREMENT EVOLVING?

Requirement 11 changed considerably during each update of the standard and there is no shortage of changes in DSS 3.0. The focus of the changes is on moving penetration testing from "dark art" to a verifiable approach that covers both applications and infrastructure, and is consistent with industry standards. This is important as penetration testing is one of the primary means of validating the status of security control effectiveness and data protection.

(See Appendix C on scoping, page 54)

Securing wireless network infrastructure
In DSS 3.0 the guidance on wireless access point security was extended to require an inventory of authorized wireless access points, each with a documented business justification (subcontrol 11.1.1). It also added a new subcontrol (11.1.2) to align with the existing testing procedure for incident response procedures if unauthorized wireless access points are detected.

Clarifying terminology
The terms "vulnerability scanning" and "penetration testing" are often misunderstood by organizations. DSS 3.0 clarifies what the standard means by these terms and uses more specific testing terminology. This will help organizations seeking compliance and the people doing the scanning to achieve a common understanding about what activities are worth including and what level of detail they should deliver.

A vulnerability assessment uses automated tools to look for known vulnerabilities across defined IP address ranges. The sorts of vulnerabilities found include unpatched or misconfigured systems.

Penetration testing goes a step further. A penetration tester — such tests will always be carried out by a person, not automated — will scan systems to identify the IP addresses, device types, operating systems and software in use. This will enable the tester to identify likely vulnerabilities, which they will try to exploit to identify and evaluate weaknesses in networks and applications. A thorough penetration test may also include using physical and social engineering techniques.

Vulnerability scanning
Since its inception the DSS has required organizations to perform quarterly vulnerability scans. DSS 1.2 introduced the need to rescan until all problems are resolved; DSS 2.0 modified this to only apply to "high" vulnerabilities (as defined in control 6.2). With DSS 3.0, additional guidance was added on combining multiple scan reports to achieve and document a passing result (control 11.2).

Penetration testing
DSS 3.0 applies a new degree of rigor to penetration testing. Subcontrol 11.3.1 in DSS 2.0 was split into two: 11.3.1 for external penetration testing and 11.3.2 for internal penetration testing.

Control 11.3 of DSS 3.0 specifies that organizations adopt a thorough, standards-based penetration-testing methodology — a best practice until July 1, 2015. Unlike Approved Scanning Vendors (ASV), who are assessed by and registered with the PCI SSC, there is no central registry, vetting, or control of companies offering penetration testing. Therefore the scope of the assessment and the quality of the report may significantly vary from one provider to another — whether performed in-house or by an external vendor. Having a defined methodology will help standardize penetration-testing activities and ensure that whatever approach the company chooses, the key points of the testing will be covered.

DSS 3.0 specifies that organizations conduct testing, regularly and after any changes, to verify that any segmentation methods used to isolate the CDE are "operational and effective" (subcontrol 11.3.4) — not just operational. These changes will increase the penetration-testing burden for organizations, but they're vital since the scope of the CDE is a foundation for the rest of the requirements.

This requirement demands that organizations actively manage data protection responsibilities by establishing, updating, and communicating security policies.

73.3%

OF COMPANIES MET ALL THE DEMANDS OF REQUIREMENT 12 IN 2013, AN INCREASE OF 43.1 PERCENTAGE POINTS ON 2012.

89.7%

IN 2013, COMPANIES WERE COMPLIANT WITH AN AVERAGE OF 89.7% OF CONTROLS.

REQUIREMENT 12

Maintain a policy that addresses information security for all personnel

WHY IS IT IMPORTANT?

Deploying security technologies such as encryption and firewalls can only go so far in protecting an organization and helping maintain compliance. Security policies address the weak link in security — users. If people don't know what's expected of them, they can put cardholder data at risk, no matter what other security measures organizations have in place.

Security policies are important because they address the weak link in security—users.

When kept up to date, documented, and formally approved, security policies play a range of important roles. Along with risk management and organizational change management, policies form the basis of a functional compliance management system and:

- Identify all stakeholders and allocate responsibility for different areas of data protection to the right people
- Communicate the intent of how and why the company protects valuable assets, including cardholder data
- Act as a reference for the standard of behavior for all security-related issues across the organization, giving:
  - Executives a mandate and framework to steer and oversee data protection programs
  - Managers a rulebook to supervise day-to-day tasks and consistently make the right decisions
  - Employees a clear view of what's expected of them

In this way, policies can make significant contribution to increasing the ROI and controlling the total cost of ownership (TCO) of an organization's PCI compliance programs.

Requirement 12's controls state that organizations must develop usage policies for critical technologies like remote access, wireless connectivity, laptops, tablets, portable storage devices, email, Internet, and more. Organizations must also clearly define security responsibilities and formally assign them to a relevant individual or team, implement an incident response plan for data breaches, and manage third-party service providers that have access to cardholder data.

Requirement 12 covers more than simply setting policies. It requires organizations to train staff regularly on data security, conduct a risk assessment at least annually, and review and update security policies at least annually.

HOW DOES THIS REQUIREMENT RELATE TO SECURITY THREATS?

When our RISK team examined a sample of more than 47,000 security incidents, it found that nearly 69% involved an insider — though often through carelessness rather than malicious intent. Of the data breaches investigated by the RISK team in 2013, just 18.2% of the victims were compliant with Requirement 12 at the time of the breach. By comparison, the average state of compliance for all organizations across the same period was 55.6%. It's clear then, that user behavior is an important factor in an organization's overall security posture.

Nearly 70% of data breaches were caused by an insider acting carelessly (though not necessarily maliciously).

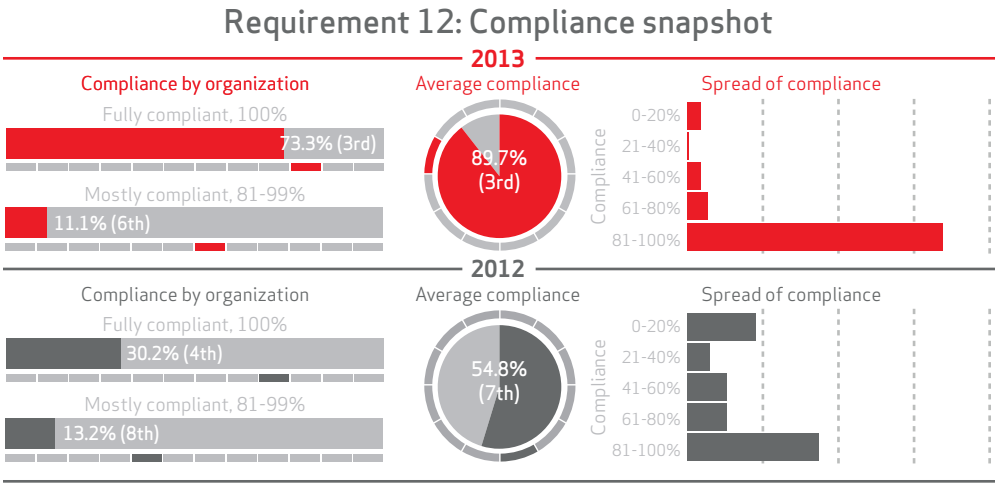


Figure 21: Snapshot for Requirement 12; dataset 2012 and 2013

Organizations found control 12.4 [Ensure that the security policy and procedures clearly define information security responsibilities for all personnel] easiest to comply with — 83.2% of organizations fulfilled all the subcontrols. This is a one-off activity that organizations will define during their initial remediation phase.

Most organizations — 79.2% and 74.3% respectively — were compliant with all the subcontrols of 12.7 [Screen potential personnel prior to hire to minimize the risk of attacks from internal sources] and 12.5 [Assign to an individual or team the following information security management responsibilities].

Organizations were less compliant with 12.1.2.b [Perform and document risk assessments at least annually] which appears in our "Bottom 20" list — only 53.5% of organizations complied.

And only 55.4% of organizations complied with 12.9.4 [Regularly train staff with security responsibilities]. Clearly, once the initial policy-setting activities are done, organizations are failing to translate compliance effort into business-as-usual activities such as training.

CHALLENGES AND PITFALLS

Policy measurement

Many organizations struggle to manage their policies effectively because they can't see who has opened and read policies, who is adhering to the policies, and so on. A poll conducted during an OCEG webinar[4] found that 90% of participants relied on systems like email, websites, document software, or content management systems for managing policies. These systems don't include metrics covering versioning, tracking, and attestations, which modern policy management systems can offer. Organizations also often fail to retain prior versions of their security policies, and are therefore unable to refer to previous versions to see when they were in effect and enforceable.

Organizations can only truly be successful at managing their data protection and compliance programs by being proactive about policy and compliance efforts, which involves active measurement of performance. Using metrics can also provide visibility into which policies users have the most questions about. This can help management to communicate the organization's data protection objectives more clearly.

Integration and change management

Many organizations do not properly integrate policy management with the business environments and support it with a change-control process. Just as changes to corporate IT architecture and processes can impact the PCI Security scope of compliance, business and technology changes can also impact security policies. Without integration, organizations find it more difficult to correlate policies with training, incidents, locations statistics, resolution rate, compliance risk assessments, and employee survey results. Leading organizations integrate compliance management into their weekly change control review meetings. Any change that may impact PCI compliance is reviewed and discussed. Such a process will help keep policies up to date.

Policies for employee-owned devices

Many organizations are struggling with "bring your own device" (BYOD) — the trend of letting employees use their own devices for business purposes, even encouraging it. Although these devices don't necessarily have access to cardholder data or form part of the PCI compliance scope, they must be considered. Policies are critically important for governing use of these devices. Control 12.3 sets out how organizations should develop and apply usage policies for this situation, including restricting access to systems and authenticating access.

Basing policies on assessed risk

To be effectively focused and practical to apply, all policies should be formulated in response to specific, identified risks. Policy generation and updating should always follow a risk assessment exercise, so that high probability and high impact risks are specifically addressed by the policies, and receive priority attention in supporting guidance documents, awareness and education. Requirement 12 covers conducting a formal risk assessment, although as we've noted earlier in this report, many argue that PCI DSS places insufficient emphasis on risk assessments, and that its guidance on what constitutes a risk assessment is too open to interpretation. In 2012, the PCI SSC responded, forming a special interest group (SIG) to produce an information supplement (pcisecuritystandards.org/documents/PCI_DSS_Risk_Assmt_Guidelines_v1.pdf) identifying several frameworks that organizations can use as a starting point. Even so, many organizations' policies are not sufficiently tailored to the results of their risk assessments.

HOW IS THIS REQUIREMENT EVOLVING?

DSS 3.0 introduced many changes to Requirement 12, including clarifications to the language, re-ordered numbering, and additional demands.

One example of a clarification is subcontrol 12.1.1. In DSS 2.0, both 12.1.1 and 12.2 covered security policies and daily procedures across all 12 requirements. DSS 3.0 includes controls for security policies and procedures that are distributed throughout each of the 12 requirements (e.g., 1.5, 2.5, 3.7, and 4.3).

There has been one addition to control 12.2 (formerly 12.1.2 in DSS 2.0) — organizations must perform risk assessments whenever there have been "significant changes" to the environment, not just annually.

There is a new subcontrol and a new control, both of which address assigning responsibility. Subcontrol 12.8.5 demands that organizations maintain information about which PCI DSS requirements are managed by which service provider, and which are managed by the organization itself. And control 12.9 orders service providers to provide a written acknowledgement to their customers if they are able to access cardholder data. This control comes into effect on July 1, 2015.

PAYMENT APPLICATION DATA SECURITY STANDARD (PA-DSS)

Payment applications are one of the weakest points in the payment chain. PA-DSS sets the standard for securing them against attack.

WHAT IS IT?

PA-DSS is a set of requirements to help software vendors develop secure payment applications that support compliance with PCI DSS. It applies to third-party applications that store, process or transmit payment cardholder data. Software applications developed in-house are exempt from PA-DSS, but must comply with PCI DSS.

By using a PA-DSS compliant application, implemented in a PCI-DSS compliant environment, a merchant only needs to follow the vendor-provided PA-DSS Implementation Guide to ensure the application and its implementation meet all applicable PCI-DSS requirements.

WHY IS IT IMPORTANT?

As a PA-DSS-compliant application must support all PCI-DSS requirements out of the box, the merchant does not need to resort to complex compensating controls in their environment. In the past payment applications might not work with anti-virus solutions, could not co-exist with new security patches in the infrastructure, or might not provide all the required logging options. From a compliance point of view, integration into the CDE should be straightforward.

During an assessment, the merchant only needs to provide evidence that the application is implemented exactly as specified by its PA-DSS Implementation Guide, which the QSA will validate. All application development requirements will be covered by the official PA-DSS Attestation of Validation provided by the vendor.

Even more important is the requirement from leading card brands that, unless developed in-house or uniquely for themselves, merchants must only use PA-DSS-validated applications in their environment.

Although this is not a requirement for PCI-DSS compliance, it forms part of many acquirers' contracts. So, not using a PA-DSS-compliant application would not stop you becoming PCI-DSS compliant; but is likely to put you in breach of contract with your acquirers.

CHALLENGES AND PITFALLS

One of the most common misconceptions is that merchants think that using PA-DSS-validated applications addresses their entire PCI-DSS compliance responsibility. It does make reaching compliance easier, and shifts the burden of complying with PCI-DSS secure application development requirements to the vendor. But, it doesn't remove the need to comply with other PCI-DSS controls applying to the environment the application is installed in.

As all PCI-DSS requirements must still be implemented in the environment, we strongly recommended that you attempt to remove CHD from your environment entirely. Switching to P2PE-validated solutions, or even just implementing tokenization, can make reaching compliance much easier than replacing an existing application with a PA-DSS-compliant one.

A common failing is using a PA-DSS-validated application but not following the relevant implementation guide. Organizations must check what environments their PA-DSS applications have been validated for, otherwise upgrading an operating system — even when demanded by PCI DSS — might render the application's PA-DSS compliance void.

Finally, merchants regularly forget that PA-DSS applies to applications installed on the payment terminals themselves. If terminal functionality is extended to include new payment channels, the additional applications installed on the terminal might need to comply with PA-DSS.

HOW IS THE PA-DSS STANDARD EVOLVING?

PA-DSS 3.0 addresses new threat vectors and alignment with the PCI-DSS standard. Noteworthy changes from PA-DSS 2.0 include:

- New subcontrol 5.2.10 addresses software development procedures to prevent broken authentication and session management. Since a flaw here could expose payment application accounts and allow session IDs to be impersonated by an attacker, this is an especially important update.
- Guidelines on the security of the development environment (controls 5.1, 5.1.5, and 5.1.6) have been updated to address new threats, particularly those affecting payment data stored in memory.
- Appreciation of security and culture at software development companies has also been addressed with a whole new requirement, 14.

The adoption of the QIR (Qualified Integrators and Resellers) program provides training and certification for resellers and integrators so that they can install payment applications following the PA-DSS implementation guide provided by the application vendor. Improper configuration has been the cause of many data compromises and using an accredited installer should help significantly reduce the risks.

FIVE WAYS TO IMPROVE YOUR PCI PROGRAM

Each year we see organizations make the same mistakes with their compliance initiatives. This is avoidable; our experience shows that the following five recommendations can help you to achieve better results.

1: DON'T UNDERESTIMATE THE EFFORT INVOLVED

Complying with PCI DSS is not easy

Organizations may transmit, process, and store cardholder data across hundreds of systems: PCs, mobile devices, web servers, databases, and point-of-sale terminals, using private and public networks, touched not only by customers but hundreds or thousands of staff. There are 289 controls that must be met in DSS 2.0, and more in DSS 3.0, and some of the individual subcontrols are potentially quite challenging to meet.

The overwhelming majority of organizations that initiate a PCI program for the first time fail to fully appreciate the impact it will have on their organization, in terms of its scope, the resources, and the time it requires. This is true even for small and mid-sized organizations with relatively simple CDEs.

Broad change demands coordination

PCI-DSS compliance requires a well-managed program comprising of many projects. It is not uncommon for a medium-sized organization to have at least 20–30 PCI projects within the initial remediation phase of its overall program. Larger organizations typically have significantly more projects — each of which must be managed and centrally coordinated to ensure overall compliance success, avoid costly mistakes, and maximize ROI.

Some organizations fail to realize this. They fail to develop the required configurations and policies, don't implement the required technologies and infrastructure, and underestimate the process and cultural change involved.

Understanding the size of the task is critical

It's common for organizations to discover several weeks, and in many cases months, down the line that they have underestimated the amount of work required to achieve PCI compliance. What they foresee as a couple of people spending a few hours each week, quickly turns out to be one or two days per week for the next 12 months — or even more.

This need not be the case. If you conduct a business impact analysis — prior to gap analysis and remediation projects — you'll get a very clear view on the impact that a PCI compliance program will have on your business. This will enable you to estimate the amount of effort required to reach compliance; in virtually all cases this is very accurate. With this calculated forecast, your CISO can confidently set to work on tackling two of the most common pitfalls we see: securing a board-level sponsor, and securing budget.

Third parties can provide essential support

Even with the best will in the world, and with sponsorship and budget secured early, your organization may lack the specialist expertise and internal resources needed. We recommend a careful, well-designed outsourcing strategy for both the management of security technologies and business processes. While using external providers clearly comes at a cost, there's a cost associated with using internal resources, too. Your choice of provider should be made not just on IT security knowledge, but on business and payment-industry knowledge as well. In many cases, a change to a business process is simpler and more effective at bringing an aspect of your business into compliance than implementing a technical solution would be.

ROOM FOR CONFUSION

Many organizations misunderstand what is and isn't in scope. Common misconceptions that we've encountered include:

"All personal data is in scope" — it's not.

"Cardholder data is out of scope if it's only stored temporarily" — it's not.

"Only systems actually within the CDE are in scope" — actually, any system that connects to the CDE, even only briefly, is in scope.

"Obfuscation of cardholder data is the same as encryption" — it's not.

"Encryption and tokenization are equivalent" — they're not.

There were eight subcontrols in our study that fewer than 50% of organizations complied with.

"Lack of education and awareness around payment security, coupled with poor implementation and maintenance of the PCI standards, gives rise to many of the security breaches happening today."

Data Security Standard and Payment Application Data Security Standard Version 3.0 Change Highlights[5]

2: MAKE COMPLIANCE SUSTAINABLE

There's no such thing as a quick fix

During the early years of PCI DSS, 2004 to 2007, it was common for organizations to see compliance as a temporary concern that could be addressed with a short-term IT project focused on adding additional technical (logical) access controls to protect cardholder data.

Our experience suggests that many companies still treat compliance as a one-off annual scramble that the security team owns and the rest of the business begrudges. Our findings emphasize that not only are companies struggling to be compliant in the first place, but also that many find it hard to maintain their compliance status year after year.

Just one new uncontrolled Wi-Fi access point, unprotected admin account, or unencrypted drive could take you out of compliance.

An increasing number of organizations are starting to realize that treating compliance as an annual fire drill is not only expensive and disruptive, but that doing so leaves them more vulnerable to non-compliance and data breaches. Just one new uncontrolled Wi-Fi access point, unprotected admin account, or unencrypted drive could take you out of compliance by the time of your next assessment — and in the meantime, your systems are vulnerable to attack.

Compliance programs must be sustainable

So what's the answer? Compliance maintenance must be an ongoing, long-term, sustainable program that's fully integrated into the day-to-day activities of the organization — "business as usual." In our experience, organizations that make this commitment are noticeably better at achieving and maintaining compliance. And we're not alone in holding this opinion: the PCI SSC and many leading analysts have highlighted the need for business culture to support risk management and compliance for many years.

It's not just about the technology

Implementing such a program means making changes to business processes and educating staff. A key part is building compliance into the corporate change-management program. For example, we recommend including PCI compliance reviews as an item in your weekly change control meetings, and allocating time to track all changes to every compliance environment, whether the changes relate to people, process, or technology. This is one of the most effective ways to manage the compliance environment, control the scope of PCI-DSS compliance, and avoid dropping out of compliance unexpectedly.

It should be an organization-wide program

You'll note that we emphasize how PCI compliance is about broad business change. Changing attitudes toward CHD must be a primary objective of your PCI program. Instead of seeing PANs and other card data as just fields in a database, every employee should be taught to see them as valuable corporate assets worthy of protection and due care. While process changes are a valuable supporting part of making this happen, success depends upon achieving cultural change, and so it's no coincidence that DSS 3.0 increases the focus on education, awareness, training and making security a shared responsibility. Compliance should not be left to your security team alone, but should also involve application developers, system administrators, executives, and even customer-facing staff in stores and call centers.

Instead of seeing PANs and other card data as just fields in a database, every employee should be taught to see them as valuable corporate assets worthy of protection and due care.

While shifting from a "fire drill" mode to regular compliance maintenance can help you to manage the workload, it's still a significant burden for all staff. Aside from the change management itself, there are activities covering patching, updates, training, and awareness as well as regular scans and tests. There are thousands of tasks that you must do throughout the year to stay compliant. You may need additional full-time people, budget, and proper oversight to avoid problems.

3: THINK OF COMPLIANCE IN A WIDER CONTEXT

PCI isn't the only tool you need

You shouldn't treat PCI Security as a blueprint for security or a checklist of everything you need to do. The catalog of controls is not sufficient to adequately protect any organization, of any size, in any sector — the same set of controls applies to the smallest café and the largest payment processor. PCI DSS should be seen as a set of minimum standards — and the PCI SSC has said as much, calling it "a compass, not a roadmap."

Just as PCI compliance is best managed by integrating it into wider organizational processes, it's also most effective when integrated into a wider security program, drawing on other tools, approaches and best practices to simplify compliance and complement its controls. DSS 3.0 includes references throughout to external standards and frameworks from the U.S. National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), and other bodies that you should use alongside the DSS to build an effective control system for protecting all your data and systems.

Think security, think intent

People often need to be reminded how important it is to consider the intent of the requirements, and the guidance for why a requirement has been created. Putting controls in place can be expensive and ineffective unless you understand the impact, and what other approaches you can take.

In particular, each control should be understood in the context of how it helps prevent a data breach, by eliminating one of the three elements that form any data breach — data, access, and egress (the "data breach triangle"[6]). For example, by limiting what is stored, you reduce the amount of data that could conceivably be breached. By identifying and closing system vulnerabilities, you can block the number of routes an attacker could use to gain access. By implementing DLP solutions, you can make the egress (exfiltration) of data harder.

The best thing you can do to simplify your PCI compliance workload is to put your PCI compliance program within your organization's larger governance, risk, and compliance (GRC) strategy. It's essential to ensure that your PCI compliance efforts support a broader control environment, and for all activities in the compliance program to be properly specified and governed in line with your unique operational environment and risk profile.

While compliance is important, you should never forget that the end goal is always to maintain effective data protection.

Time and money invested in data protection and compliance should meet clear objectives. The outcome of each activity should be to establish ongoing, sustainable protection of data, not just to meet periodic compliance requirements.

4: LEVERAGE COMPLIANCE AS AN OPPORTUNITY

What can compliance do for you?

We advocate that compliance-mature organizations stop looking at PCI compliance as a cost of doing business, and instead see it as an investment to be leveraged. Compliance forces you to take a long hard look at your systems and processes in order to map all CHD flows across systems and processes. The understanding that this gives is not just vital for compliance, but can also give you fantastic insight into your business that can help you identify areas for improvement. You could identify opportunities to:

- Consolidate systems, not only reducing scope but cutting your software licensing, maintenance and facilities costs
- Rationalize your list of suppliers and clarify roles and responsibilities
- Transform or streamline outdated processes and reduce staffing
- Improve system performance and uptime by better applying patches and configuration best practices
- Consolidate existing merchant contracts with your acquiring banks and payment processors to achieve better transaction fees

In these ways, activities undertaken for compliance purposes can not only protect your reputation and save you from fines and damage to your reputation, but also help generate ROI.

Don't just measure TCO, measure ROI, too

Research we conducted in 2013[7] found that, although some organizations calculate the TCO of their compliance programs, very few of them take the next step and calculate or even estimate the ROI.

This lack of insight into the overall impact of the compliance program places compliance officers at a major disadvantage. Complete transparency is required to obtain genuine support from the business. And more importantly, complete visibility and clarity is crucial in order to determine how changes in the compliance industry, such as updates to the PCI standards, evolving threats to sensitive data, or innovation in payment card industry technology might impact your business's sustainability and profitability.

5: FOCUS ON SCOPING

The foundation of an effective PCI program is a clear definition of the systems, processes, and people that store, process, or access cardholder data. The scope is defined by the organization itself and assessed by the QSA (or ISA) during validation.

There are three good reasons to reduce the scope of the environment to be validated:

- **Reducing risk:** By minimizing the spread of cardholder data across your organization you can limit the risk of data leaking or being stolen, and you can minimize the scale of any breach that should happen. Creating designated "compartments" between the various networks within an organization helps categorize and securely contain business data. This reduces the likelihood that a data breach can spread throughout your organization's IT infrastructure — according to the 2013 DBIR, 78% of data breaches take weeks, months or even years to be discovered, giving hackers plenty of time to hunt around for what they're after.
- **Reducing workload:** From a practical perspective, effective scoping can help you to significantly cut your compliance workload. Any system that is validated as "out of scope" doesn't need to be assessed (it is regarded as outside of the CDE, so none of the requirements of PCI DSS apply to it). This is crucial, because complying with all of the requirements of the PCI DSS across an entire business, even a small one with a relatively simple infrastructure, can be a challenging task; the workload would be too great.
- **Controlling operating costs:** Scoping forces you to take a long, hard look at your infrastructure. While you're making changes to reduce scope, you may find that you can consolidate systems and restructure environments, saving money on hardware, software licenses, and management along the way.

See Appendix C on scoping on page 54.

CONCLUSION

2014 is likely to be an interesting year for PCI compliance. As well as the impact that DSS 3.0 will no doubt have on the state of compliance and the debates around scoping, risk management and other important areas, we also expect to see broader use of P2PE — perhaps the most important opportunity in years (for merchants at least) to simplify their PCI compliance burden.

We hope that subsequent releases of this report will document how well the compliance landscape is evolving. But whatever the future holds, we will continue to engage with the PCI Security community to improve the program, and we welcome your input and feedback.

Questions? Comments? We want to hear them. Drop us a line at pcireport@verizon.com, find us on linkedin.com/company/verizon-enterprise or tweet us @VzEnterprise with the hashtag #pcireport.

Appendix A
DEFINITION OF KEY TERMS

ACCOUNT DATA
Cardholder data plus sensitive authentication data.

ACL
Access control list.

ASV
Authorized scanning vendor.

BASELINE ASSESSMENT
An interim compliance validation assessment performed by a QSA to determine the PCI Security compliance status.

CDE
Cardholder data environment — all people, processes, and technologies that store, process, or transmit CHD or SAD.

CHD
Cardholder data.

CISO
Chief Information Security Officer.

CVSS
Common Vulnerability Scoring System.

CVV/CVV2
Card verification value. Both of these terms are commonly used to refer to the number printed on a card to help secure "card not present" transactions — other terms include CVC, CID and CSC. To be precise, the code printed on the card is actually the CVV2 — and the CVV is integrity-check data encoded on the magnetic strip — but both terms are widely used online.

DBIR
Data Breach Investigations Report (verizonenterprise.com/dbir).

DLP
Data loss prevention solution — a system that restricts the transmission of sensitive data, reducing the risk of suffering a breach

DMZ
Demilitarized zone.

DSS
PCI Data Security Standard.

EMV
Europay/MasterCard/Visa, the standard for credit and debit payment cards based on chip card technology — commonly known as "Chip and PIN."

FROC
Final report on compliance.

FULL ISOLATION
This method has been interpreted as no communication whatsoever between any component in the CDE and any non CDE, regardless of which device initiates the connection, and whether the communication channel is secure and is established between trusted systems.

Isolation is achieved using various methods, including:
- "Deny all" rules on routers and firewalls
- Host-based network and application access restriction
- Physical "air gap" isolation

Due to lack of clarity, many organizations within the PCI community question the practical sustainability of a "full isolation model" in complex, large-scale environments – depending on their wide-ranging interpretations.

GRC
Governance, risk and compliance.

IOC
Indicator of compromise. RSA, the security division of EMC, defines an IOC as "a forensic artifact or remnant of an intrusion that can be identified on a host or network."

IPS
Intrusion prevention system.

IROC
The output of a baseline assessment, details the changes required to address deficiencies.

ISA
Internal security assessor.

NTP
Network time protocol.

OWASP
Open Web Application Security Project.

P2PE
Point-to-point encryption. See Appendix B on page 53.

PA-DSS
Payment Application Data Security Standard.

PAN
Primary account number.

PARTIAL ISOLATION OF CHD
See Trusted Communication.

PCI
Payment card industry.

PII
Personally identifiable information.

PIM
P2PE implementation manual.

PIN
Personal identification number.

POI
Point of interaction.

PTS
PIN transaction security.

QIR
Qualified Integrators and Resellers, a PA-DSS program.

QSA
Qualified security assessor.

ROC
Report on compliance.

SAD
Sensitive authentication data.

SAQ
Self-assessment questionnaire.

SEGMENTATION
Segmentation splits (partitions) networks at a logical layer, dividing one part of a network from another; typically using firewall access control, router and firewall combination, VLANs with access control lists (ACLs).

SEGREGATION
Effective system segregation can be achieved using a combination of methods, such as port restriction, communication protocol restriction, IP address restriction, and application-level restriction. Segregation is normally used to create divisions between devices, not networks.

TOKENIZATION
The principle of tokenization is to remove the PAN from as many internal systems as possible, and replace it with a different, but similarly unique, piece of data — the token. The potential advantages include:

- Very little or no recoding of the applications that use the token in place of the PAN
- Fast deployment — either all at once, or phased
- Low cost — the only major cost is acquiring or developing the tokenization solution

But what seems to be the panacea on paper can become daunting in reality. In order to be regarded as out of scope, tokens and the systems must have no value to an attacker attempting to retrieve PAN, or impact the security of the CDE in any way. Specifically:

- Both the tokens and the systems they reside on must be evaluated to determine whether they should be in scope
- Any systems connected to the tokenization or detokenization system remain in scope

Despite significant improvements in tokenization solutions over the last couple of years, the use within the CDE still requires careful deployment and a clear management strategy. It's not a panacea.

For more information on tokenization, see the PCI guidelines: pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf.

TRUSTED COMMUNICATION
There are calls for formal approval and specification of a "trusted communication" or "partial isolation" model. This could combine segmentation and segregation methods to restrict communication between CDE and systems in a controlled, and specifically defined manner depending on the direction and type of communication. We believe that such a model would support existing approaches to secure network communication, like the "Zero Trust" model from Forrester.[8]

In this model, network connections are initiated and/or received from trusted system components only. Internal networks and internal network segments are not trusted by default, but only trusted when validated as such (i.e., "zero trust").

The partial isolation of CHD relies on controlled access using a combination of (network) segmentation and (system component) segregation. Trusted systems in trusted networks can initiate secure, controlled communication to specific systems in untrusted networks, but not vice versa. Untrusted systems and networks cannot initiate any communication to CHD or other trusted environments.

There is no direct access into a CDE from an untrusted network, and no direct link initiated from a CDE to any untrusted network.

Compared with full isolation, this model may require more maintenance, and more comprehensive policies and procedures.

SIEM
Security information and event management system.

SIG
Special interest group

SSC
PCI Security Standards Council

SSL/TLS
Secure sockets layer/transport layer security

VERIS
Vocabulary for Event Recording and Incident Sharing — a structured framework for describing security incidents. For more information see veriscommunity.net.

Appendix B

POINT-TO-POINT ENCRYPTION (P2PE)

Any system that transmits, processes or stores encrypted PANs remains in scope of the PCI DSS, if the organization has the ability to decrypt the data. The idea behind P2PE is to remove that ability, and therefore simplify the compliance requirements for that system. Under P2PE, cardholder data is encrypted as soon as it enters a payment system at the POS terminal and remains encrypted all the way through the merchant's environment. The data is only decrypted once it has been safely and securely transported to the acquirer or payment processor. The payment processor takes responsibility for cryptographic key management and PCI compliance, and the merchant never has access to the keys — and hence the unencrypted data.

P2PE can also help merchants manage the diversification of their payment infrastructures. Today customers expect seamless integration of the retail experience across all available shopping channels — online, in-store, telephone, etc. — known as omnichannel. This is putting organizations under pressure to take payments through tablets and smartphones, kiosks and self-service terminals, as well as standard payment terminals. Without some measure to take some or all of these different channels out of scope, PCI compliance would be extremely difficult to achieve.

In October 2013, the PCI SSC validated its first hardware-based solution. The SSC has a large task force working on software-based P2PE, and guidance on requirements and implementation is expected in 2014. However, software-based P2PE is widely viewed as more vulnerable to tampering in a retail or hospitality environment where transactions may be unattended by a cashier.

We are seeing more and more interaction between PA-DSS, PCI DSS, PTS, PCI PIN, and P2PE standards. For example, PCI DSS 3.0 subcontrol 3.5.2, which specifies how and where encryption keys should be stored, directly mirrors P2PE requirement 6F-1.1. Moreover, in order to introduce some basic P2PE principles into DSS 3.0, the SSC has added control 9.9, which is related to protecting card terminals from tampering and substitution.

P2PE doesn't entirely remove or replace all PCI-DSS obligations. Organizations must ensure that the P2PE environment is properly segmented from any other payments channels (e.g., ecommerce), and these other channels must be validated. And even fully validated P2PE implementations can still have a number of components within the CDE that would remain in scope and need to be evaluated against PCI DSS to keep the system secure and maintained.

P2PE is still not widely deployed, partly due to a lack of suitable approved solutions — these are only now appearing on the market.

Challenges for merchants: Getting P2PE up and running can include upgrades to POS hardware and software; and increased fees from vendors ready to take advantage of businesses trying to reduce their compliance obligations. This can represent a sizeable financial investment. Another major difficulty is following the solution provider's P2PE implementation manual (PIM), especially the device management process implementation. It can be cumbersome to track and protect devices effectively.

Challenges for solution providers: Achieving P2PE validation won't necessarily be easy even for PCI-DSS-validated organizations using PTS-validated point of interaction (POI) — there's a whole new set of requirements to comply with. As a result, providers must make sure they allow sufficient time and resources, and follow the same structure as in any assessment: define the scope of the solution, perform a gap analysis, and then develop a remediation plan.

Requirements covering third-party relationships, security policies, the education of staff handling account data, and physical security of media still apply to merchants that have implemented a validated P2PE solution.

Appendix C
SCOPING

Faced with the challenge of making important decisions on scoping under conditions of uncertainty, QSAs and complying organizations have come up with diverging interpretations.

Clarifying definitions

There is a lack of consensus within the PCI Security industry on the definitions around scoping and what scope-reduction methods are approved. This is a critical issue because any scoping project must start with understanding the definitions and agreeing on the terminology.

The terminology around scope-reduction methods is somewhat inconsistent and clear guidance is needed to correct the many misunderstandings. The terms "isolation" and "segmentation" are used interchangeably in PCI DSS 3.0, but they should be treated as distinct concepts. Also, the term "segregation" is not used, but is a more appropriate term in many cases. The concept of full isolation may indeed reduce the risk and enhance the protection of payment card data; however, it seemingly contributes to the lack of clarity and uncertainty within the industry around scoping and permissible scope-reduction methods.

We, along with many others, interpret the PCI SSC guidance as saying that only isolation fully removes a system from scope, but in practice this kind of full isolation can be impractical.

One of 2013's largest breaches targeted a leading software company. Not only did hackers compromise the CHD of three million customers, they also took registration data from 38 million users and source code from several of its flagship applications. Increasingly criminals are using biographical data gained from multiple sources to perpetrate more and larger thefts. This can be as simple as using address information to keep fraudulent transactions local, reducing the likelihood of triggering anti-fraud systems. Obviously no data breach is good news, but the less that the criminals can take, the less the damage to your company's reputation is likely to be.

APPROACHES TO SCOPE REDUCTION

You can reduce the scale of your compliance project by storing less data in fewer places. To follow best practice, don't retain any payment card data when there is not a clear, demonstrable business need to do so. Excessive retention of data is both costly from a data protection perspective, and it also increases the business risk associated with the data.

But there's only so far that you can go to minimize what data you store. The other way to reduce scope is by separating the systems and processes that touch cardholder data from those that don't. Primarily, it's about segmentation. Many organizations already segment their networks for performance, manageability, business continuity, and security reasons — but how does it work in a compliance sense?

Scoping is a significant activity that should be undertaken not only before the first validation, but regularly. It should involve not just technical considerations, but business processes, too.

PCI-DSS remediation and validation assessment projects require formal analysis and examination of the entire operational card data environment to be conducted early in the project. This should be followed by the precise definition and full documentation of the company's scope of compliance.

Prior to, during and after each gap analysis; prior to the annual assessment; and at least annually, you should confirm the accuracy of your PCI-DSS scope by identifying all locations and flows of CHD to verify that no cardholder data exists outside of your currently defined CDE.

OUT OF SCOPE, BUT NOT OUT OF MIND

While reducing the scope of your PCI cardholder data environment is great from a workload point of view — and so a hugely tempting proposition — criminals don't care about your scoping definitions. It's not just cardholder data that's important; criminals are also after other personally identifiable information (PII) and corporate data. Systems may be out of scope, but they can still contain important data, host business-critical applications, and offer hackers some way of getting access to CHD.

The CDE comprises all people, processes, and technologies that store, process, or transmit CHD or sensitive authentication data.

Related systems that connect to the CDE also fall within the scope of compliance and need to be evaluated, documented on hardware and software lists and network diagrams, and monitored. They will be assessed for compliance. Excluded environments require documentation and verification, too.

As well as the results, you should retain documentation that shows how your PCI-DSS scope was confirmed for assessor review and/or for reference during the next annual PCI-DSS scope confirmation activity.

We recommend that organizations define, implement, and maintain a process to proactively manage the scope of compliance for each environment. Discussions about scope reduction and management are often a daily event between QSAs and their clients.

"Segmentation can be achieved through a number of physical or logical means, such as properly configured internal network firewalls, routers with strong access control lists, or other technologies that restrict access to a particular segment of a network."

PCI Data Security Standard 3.0, November 2013, p11

CHALLENGES OF SCOPE REDUCTION: CONTACT CENTER

Some organizations, particularly those complying for the first time, find that some PCI requirements have unforeseen and frustrating effects on particular business functions and processes. The contact center is a case in point. The additional challenge in this environment, compared to transactions carried out face-to-face (cardholder present), is that nearly everybody in a contact center has the ability to listen to recorded telephone calls. If these contain CHD, the threat of a data breach becomes obvious. PCI DSS requires that sensitive authentication data not be stored in call recordings, and recommends isolating contact center agents from CHD where possible.

Many organizations struggle to see a way to take CHD out of calls, call recordings and agent screens without major disruption to infrastructure, customers, or agent workflows. But with a little creativity — which an experienced advisor can provide — there are options. Some can even remove the entire contact center from scope, which can offer huge benefits. For example, it's possible to use an onsite or offsite system to capture card details entered directly via the caller's phone keypad. Card details are never read out to the agent or recorded, therefore eliminating risk and reducing DSS scope. Such systems can be costly and require extensive integration, but produce savings by taking the contact center out of scope. And they're much less disruptive than transferring callers to an interactive voice response (IVR) system or other separate channel at the time of payment. The conversation with the agent can continue uninterrupted.

See Appendix A for definitions of some key scoping and other PCI-related terms, page 51.

ABOUT VERIZON'S PCI SECURITY PRACTICE

Verizon is a highly respected security provider with a depth of insight into PCI compliance.

In the world of IT security, knowledge is power. That's why we work tirelessly to extend and deepen our expertise, through our long-running commitment to research, the unique insights we gather by running one of the largest global IP networks, and acquisitions of leading security companies such as Cybertrust.

Today, Verizon is one of the most trusted voices in the PCI Security community. And with good reason: we have one of the largest QSA teams in the world, and over 550 security professionals globally. This means that we have an unrivalled perspective into the experiences that organizations in all kinds of industries and countries encounter during their governance, risk, and compliance programs. The figures from our PCI team speak for themselves. We've conducted more than 4,000 assessments for 500 client organizations, many of which are large multinationals. In total, we've assessed more than 750,000 individual validation testing requirements.

We put this depth of experience to work for clients in three main areas:

- **Assessment and maintenance:** through PCI Security assessments we review and validate customers' compliance, and then through our PCI compliance maintenance program we help them stay that way. We also offer vulnerability scanning services to meet the demands of the DSS.
- **Remediation:** we offer a range of targeted remediation solutions, drawing on the full range of Verizon security products and services, to provide a cost-effective way to comply.
- **Outsourcing:** Verizon's range of hosting and cloud services and managed security services take the burden of running, maintaining and securing key IT services, helping make compliance easier.

As well as being experts in PCI Security standards, our consultants and assessors have deep industry knowledge, often gained through years of experience working directly within retail, hospitality, financial services, healthcare and other sectors. This knowledge means we truly appreciate your challenges, put PCI Security in the context of your industry-specific regulations and standards, and make recommendations not just in terms of IT change, but business process transformation, too.

For additional resources on this research and to find out more about Verizon's PCI Security compliance services, please visit verizonenterprise.com/pcireport/2014.

VERIZON PCI SECURITY PRACTICE

MANAGING DIRECTOR
Rodolphe Simonetti

MANAGEMENT TEAM
Aaron Reynolds
Andi Baritchi
Auro Gaudeni
Ciske van Oosten
Gabriel Leperlier
Ian White
Kim Haverblad
Sebastien Mazas

1. http://www.theguardian.com/world/2014/jan/23/fbi-warns-retailers-cyber-attacks-target-breach

2. http://www.imperva.com/docs/HII_Assessing_the_Effectiveness_of_Antivirus_Solutions.pdf

3. https://security.berkeley.edu/content/what-difference-between-vulnerability-scan-and-penetration-test?destination=node/195

4. http://www.oceg.org/event/the-2012-grc-maturity-survey-report/

5. https://www.pcisecuritystandards.org/documents/DSS_and_PA-DSS_Change_Highlights.pdf

6. https://securosis.com/blog/the-data-breach-triangle/

7. Verizon 2013 PCI Security Survey, 2013

8. Forrester Research, Inc., No More Chewy Centers: Introducing The Zero Trust Model Of Information Security, November 2012, http://www.forrester.com/No+More+Chewy+Centers+Introducing+The+Zero+Trust+Model+Of+Information+Security/fulltext/-/E-RES56682?objectid=RES56682